S. HRG. 107–1086

JOINT INQUIRY INTO INTELLIGENCE COMMUNITY ACTIVITIES BEFORE AND AFTER THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001

HEARINGS

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE U.S. SENATE

AND THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE HOUSE OF REPRESENTATIVES

VOLUME II

OCTOBER 1, 3, 8, AND 17, 2002

U.S. GOVERNMENT PRINTING OFFICE

96–167 WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SENATE SELECT COMMITTEE ON INTELLIGENCE

107TH CONGRESS

BOB GRAHAM, Florida, *Chairman*
RICHARD C. SHELBY, Alabama, *Vice Chairman*

CARL LEVIN, Michigan
JOHN D. ROCKEFELLER, West Virginia
DIANNE FEINSTEIN, California
RON WYDEN, Oregon
RICHARD J. DURBIN, Illinois
EVAN BAYH, Indiana
JOHN EDWARDS, North Carolina
BARBARA MIKULSKI, Maryland

JON KYL, Arizona
JAMES M. INHOFE, Oklahoma
ORRIN HATCH, Utah
PAT ROBERTS, Kansas
MIKE DEWINE, Ohio
FRED THOMPSON, Tennessee
RICHARD LUGAR, Indiana

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

107TH CONGRESS

PORTER J. GOSS, Florida, *Chairman*
NANCY PELOSI, California, *Ranking Democrat*

DOUG BEREUTER, Nebraska
MICHAEL N. CASTLE, Delaware
SHERWOOD L. BOEHLERT, New York
JIM GIBBONS, Nevada
RAY LAHOOD, Illinois
RANDY "DUKE" CUNNINGHAM, California
PETER HOEKSTRA, Michigan
RICHARD BURR, North Carolina
SAXBY CHAMBLISS, Georgia
TERRY EVERETT, Alabama

SANFORD D. BISHOP, Georgia
JANE HARMAN, California
GARY A. CONDIT, California
TIM ROEMER, Indiana
SILVESTRE REYES, Texas
LEONARD L. BOSWELL, Iowa
COLLIN C. PETERSON, Minnesota
BUD CRAMER, Alabama

CONTENTS

Volume II

Page

Hearing held in Washington, D.C., October 1, 2002 1

Testimony of:

Andre, Louis, Special Assistant for Intelligence, J–2, Defense Intelligence Agency 164

Gilmore, James III, Chairman, Advisory Panel to Assess Domestic Response Capabilities for Terrorism 107

Greene, Joseph, Assistant Commissioner for Investigations, U.S. Immigration and Naturalization Service 158

Hill, Eleanor, Staff Director, Joint Inquiry Committee 75

Manno, Claudio, Assistant Under Secretary for Intelligence, Transportation Security Administration 150

Norris, Edward T., Commissioner of Police, City of Baltimore 167

Taylor, Ambassador Francis X., Coordinator for Counterterrorism, Department of State 139

Supplemental Materials:

Statement for the Record of Hon. Spencer Abraham, Secretary, Department of Energy, dated September 20, 2002 231

Responses to QFRs from the Central Intelligence Agency 241

Responses to QFRs from the Defense Intelligence Agency 248

Responses to QFRs from the Department of State 255

Statement of David M. Walker, Comptroller of the United States 3

Statement for the Record by Rear Admiral Lowell E. Jacoby, USN, Acting Director, Defense Intelligence Agency 53

Statement of Dr. Robert C. Norris, Jr., Chair, Information Operations and Technology Department, National Defense University 60

Hearing held in Washington, D.C., October 3, 2002 263

Statement of:

Hamilton, Hon. Lee H., Director, Woodrow Wilson International Center for Scholars, Indiana University 278

Hill, Eleanor, Staff Director, Joint Inquiry Committee 266

Hitz, Frederick, Director, Project on International Intelligence and Lecturer of Public and International Affairs, Princeton University 303

Odom, Lieutenant General William E. Ret., Director, National Security Studies, Hudson Institute 294

Webster, Hon. William, Chairman, Webster Commission 290

Supplemental Materials:

August 27, 2002 Letter from DCI George Tenet to Senator Dianne Feinstein 345

October 11, 2002 Memorandum from William E. Odom to Senator Dianne Feinstein 362

October 11, 2002 Letter from Lee H. Hamilton to Mr. Robertson 364

Hearing held in Washington, D.C., October 8, 2002 365

Testimony of:

Fallis, Kie, Intelligence Consultant 582

Freeh, Hon. Louis, Former Director, Federal Bureau of Investigation 449

Hill, Eleanor, Staff Director, Joint Inquiry Committee 368

Pillar, Paul R., National Intelligence Officer for the Near East and South Asia and Former Deputy Chief, Counterterrorist Center, Central Intelligence Agency 558

Rudman, Hon. Warren, Former U.S. Senator from the State of New Hampshire 444

Page

Testimony of—Continued
White, Mary Jo, Former U.S. Attorney for the Southern District of N.Y. ... 495
Supplemental Materials:
Listing of proposals for Intelligence Reorganization, 1990–Present 615
Selected Events in the Chronology of Terrorism, 1982–2001 395
Statement of Dr. Bruce Hoffman, Vice President, External Affairs and Director, Rand Corporation, August 20, 2002 413
Declassified findings and recommendations from the Senate Select Committee on Intelligence inquiry into intelligence collection, reporting, analysis and warning relevant to the bombing of the USS *Cole* 441

Hearing held in Washington, D.C., October 17, 2002 619
Testimony of:
Hayden, Lieutenant General Michael V., USAF, Director, National Security Agency 784
Hill, Eleanor, Staff Director, Joint Inquiry Committee 672
Mueller, Hon. Robert, Director, Federal Bureau of Investigation 748
Tenet, Hon. George J., Director of Central Intelligence 704
Statement of:
Clapper, Lieutenant General James R., USAF, Ret., Director, National Imagery and Mapping Agency 687
Jacoby, Rear Admiral Lowell E., U.S. Navy, Acting Director, Defense Intelligence Agency 696
Supplemental Materials:
August 22, 2002 Letter from International Association of Chiefs of Police to Robert Mueller, Director of the Federal Bureau of Investigation 766
December 20, 2001 Letter from Maryland Chiefs of Police Association to Robert Mueller, Director of the Federal Bureau of Investigation 768
May 1, 2002 Letter from New York State Police to Robert Mueller, Director of the Federal Bureau of Investigation 770
June 14, 2002 Letter from Orange County Sheriff's Office to Robert Mueller, Director of the Federal Bureau of Investigation 772
June 24, 2002 Letter from Institute for Intergovernmental Research to Robert Mueller, Director of the Federal Bureau of Investigation 774
July 25, 2002 Letter from Chief of Police, Town of Cary, to Robert Mueller, Director of the Federal Bureau of Investigation 777
August 29, 2002 Letter from Omaha Police to Robert Mueller, Director of the Federal Bureau of Investigation 779
August 5, 2002 Letter from City of Orlando to Robert Mueller, Director of the Federal Bureau of Investigation 780
List of CIA and FBI Failures prepared by Senator Carl Levin 810
Expanded version of Eleanor Hill statement of September 24, 2002 647
June 18, 2002 declassified statement of George J. Tenet, Director of Central Intelligence 626

JOINT COMMITTEE HEARING ON COUNTER-TERRORISM INFORMATION-SHARING WITH OTHER FEDERAL AGENCIES AND WITH STATE AND LOCAL GOVERNMENTS AND THE PRIVATE SECTOR IN REVIEW OF THE EVENTS OF SEPTEMBER 11, 2001

TUESDAY, OCTOBER 1, 2002

U.S. SENATE, SELECT COMMITTEE ON INTELLIGENCE AND U.S. HOUSE OF REPRESENTATIVES, PERMANENT SELECT COMMITTEE ON INTELLIGENCE,

Washington, D.C.

The Committees met, pursuant to notice, at 10:15 a.m., in Room 216, Hart Senate Office Building, the Honorable Bob Graham, Chairman of the Senate Select Committee on Intelligence, presiding.

Senate Select Committee on Intelligence Members Present: Senators Graham, Shelby, Rockefeller, Feinstein, Wyden, Mikulski, Roberts, and DeWine.

House Permanent Select Committee on Intelligence Members Present: Representatives Goss, Boehlert, Gibbons, Hoekstra, Burr, Pelosi, Bishop, Harman, Roemer, Boswell, Peterson and Cramer.

Chairman GRAHAM. I call to order the Joint Inquiry of the House and the Senate Select Committee on Intelligence. This is the sixth open hearing by our committees as we consider our joint inquiry into the Intelligence Community's performance regarding the September 11 tragedies. During the course of our investigation, we have considered questions about the sharing of information among the major parts of our intelligence community, the CIA, NSA and the FBI, as well as between law enforcement and the intelligence components, particularly of the FBI. Today we will focus on several other aspects of information sharing.

One is the sharing of information between the principal elements of the Intelligence Community and a range of Federal agencies, such as the Federal Aviation Administration and the Immigration and Naturalization Service, which are important users of intelligence information and which also may generate intelligence information of use to others.

A second issue is the sharing of intelligence information between the Federal Government and State or local governments as well as parts of the private sector. To discuss these two issues this morning, we will have a staff report by our staff director, Ms. Eleanor Hill, and then a panel. The panel will include the Honorable James

S. Gilmore, III, former Governor of the Commonwealth of Virginia and chairman of the Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism involving weapons of mass destruction; Ambassador Francis X. Taylor, coordinator for counterterrorism at the Department of State; Mr. Claudio Manno, acting Associate Under Secretary for Intelligence at the Transportation Security Agency; Mr. Joseph B. Greene, Assistant Commissioner for Investigations, U.S. Immigration and Naturalization Service; Mr. Louis E. Andre, Special Assistant to the Director for Intelligence, J–2 of the Defense Intelligence Agency; and Edward T. Norris, Police Commissioner for the City of Baltimore.

Additionally, the committee has received three statements for the record that will be—that will not be accompanied by oral testimony. These three statements for the record are by David M. Walker, Comptroller General of the United States, Rear Admiral Lowell Jacoby, acting director, Defense Intelligence Agency; and Robert C. Norris, Jr., Chair Operations Information Technology Department of the National Defense University.

I ask unanimous consent that each of these statements be made part of the record of this hearing.

Chairman GOSS. So move, Mr. Chairman.

[The prepared statements of Mr. Walker, Admiral Jacoby, and Mr. Norris follow:]

United States General Accounting Office

GAO

Testimony

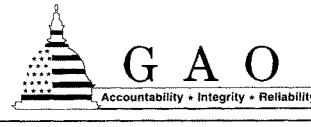
Before the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, U.S. Congress

Statement for the Record
September 23, 2002
For Release on
October 1, 2002

HOMELAND SECURITY

Information Sharing Activities Face Continued Management Challenges

Statement of David M. Walker
Comptroller General of the United States



GAO-02-1122T

Messrs. Chairmen and Members of the Committees:

Since the September 11, 2001, terrorist attacks, both the Administration and Congress have focused on the performance of the intelligence community and whether intelligence and other information is effectively shared – between federal agencies, with state and local law enforcement and other officials, and with private entities – to prevent or respond to terrorist attacks. Both the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have, in their joint inquiry, helped to illuminate many issues from which lessons can be drawn to improve how our intelligence community and other homeland security stakeholders share, analyze, integrate and disseminate important information, both at home and overseas.

Today, governments at all levels, as well as private sector entities, recognize that they have a greater role to play in protecting the nation from terrorist attacks. To achieve this collective goal, homeland security stakeholders must more effectively work together to strengthen the process by which critical information can be shared, analyzed, integrated and disseminated to help prevent or minimize terrorist activities. The work of these committees and of others in Congress and the Administration in crafting solutions to leverage agencies' abilities and willingness to share timely, useful information is critical to the fundamental transformation required in our homeland security community to ensure an affordable, sustainable and broad-based response to new and emerging threats to our country.

In your request that GAO provide a statement for the record, you asked us to focus on the information sharing activities of the intelligence, law enforcement, and other agencies involved in homeland security, as well as the role of state and local governments and the private sector. You also requested that we provide a description and status of the principal recommendations we have made related to combating terrorism.

We have developed an extensive body of work on combating terrorism over the years and more recently we have issued a number of reports on homeland security. Based on GAO's *Strategic Plan* issued in January 2000, which included a new emphasis on addressing key emerging threats to national security in a post-Cold War environment, GAO issued many reports prior to September 11th on combating terrorism and related matters. At the request of Congress, or on our own initiative, we currently have more than 80 engagements under way to examine a variety of

homeland security issues. Our ongoing work includes evaluations of information sharing activities in homeland security, including reviews of airport and transportation security, seaport security and law enforcement agencies. However, as the committees are aware, GAO's work in evaluating the activities of the intelligence community historically has been limited, due in part to limitations imposed by the intelligence agencies and the small number of requests made by Congress. My statement today reflects this limitation on evaluations of the intelligence community and focuses more broadly on information sharing among various homeland security stakeholders.

In my testimony today, I will discuss (1) some of the challenges to effective information sharing, including the fragmentation of information analysis responsibilities, and technology and collaboration challenges, and (2) GAO's views on addressing these challenges through transformational strategies, including strengthening the risk management framework; refining the national strategy, policy, and guidance structures to emphasize collaboration and integration among homeland security stakeholders to achieve common goals; and bolstering the fundamental management foundation integral to effective public sector performance and accountability. The statement also includes an appendix that lists GAO's recommendations on combating terrorism and the status of their implementation, as well as a list of related products.

Challenges to Effective Information Sharing

The success of a homeland security strategy relies on the ability of all levels of government and the private sector to communicate and cooperate effectively with one another. Activities that are hampered by organizational fragmentation, technological impediments, or ineffective collaboration blunt the nation's collective efforts to prevent or minimize terrorist acts.

Information Sharing Fragmentation

GAO and other observers of the federal government's organization, performance, and accountability for combating terrorism and homeland security functions have long recognized the prevalence of gaps, duplication, and overlaps driven in large part by the absence of a central policy focal point, fragmented missions, ineffective information sharing, human capital needs, institutional rivalries, and cultural challenges. In recent years, GAO has made numerous recommendations related to changes necessary for improving the government's response to combating terrorism.[1] Prior to the establishment of the Office of Homeland Security (OHS), GAO found that the federal government lacked overall homeland security leadership and management accountable to both the President and Congress. GAO has also stated that fragmentation exists in both coordination of domestic preparedness programs and in efforts to develop a national strategy.[2]

GAO believes that the consolidation of some homeland security functions makes sense and will, if properly organized and implemented, over time lead to more efficient, effective, and coordinated programs, better information sharing, and a more robust protection of our people, borders, and critical infrastructure.[3] At the same time, even the proposed Department of Homeland Security (DHS), will still be just one of many players with important roles and responsibilities for ensuring homeland security. In addition, the creation of DHS will not be a panacea. It will create certain new costs and risks, which must be addressed.

As it is with so many other homeland security areas, it is also the case for intelligence and information sharing that there are many stakeholders who must work together to achieve common goals. Effective analysis, integration, and dissemination of intelligence and other information critical to homeland security requires the involvement of the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), the National Security Council (NSC), the National Security Agency (NSA), the Department of Defense (DOD), and a myriad of other agencies, and will also include the

[1]U.S. General Accounting Office, *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington, D.C.: September 2001).

[2]U.S. General Accounting Office, *Combating Terrorism: Comments on Counterterrorism Leadership and National Strategy*, GAO-01-556T (Washington, D.C.: March 27, 2001).

[3]U.S. General Accounting Office, Homeland Security: Critical Design and Implementation Issues, GAO-02-957T (Washington, D.C.: July 17, 2002).

proposed DHS. State and local governments and the private sector also have critical roles to play – as do significant portions of the international community. Information is already being shared between and among numerous government and private sector organizations and more can be done to facilitate even greater sharing, analyzing, integrating, and disseminating of information.

We have observed fragmentation of information analysis and sharing functions potentially requiring better coordination in many homeland security areas. For example, in a recent report on critical infrastructure protection (CIP), we indicated that some 14 different agencies or components had responsibility for analysis and warning activities for cyber CIP.[4] Onr recent testimony on aviation security indicated that the Immigration and Naturalization Service (INS), FBI and the Department of State all need the capacity to identify aliens in the United States who are in violation of their visa status, have broken U.S. laws, or are under investigation for criminal activity, including terrorism.[5] GAO has also noted that information sharing coordination difficulties can occur within single departments, such as those addressed in our July 2001 review of FBI intelligence investigations and coordination within the Department of Justice.[6] Procedures established by the Attorney General in 1995 required, in part, that the FBI notify the Criminal Division and the Office of Intelligence Policy and Review whenever a foreign counterintelligence investigation utilizing authorized surveillance and searches develops "...facts or circumstances...that reasonably indicate that a significant federal crime has been, is being, or may be committed...." However, according to Criminal Division officials, required notifications did not always occur and often, when they did, were not timely. The Attorney General and the FBI issued additional procedures to address the coordination concerns and ensure compliance, but these efforts have not been institutionalized.

[4] U.S. General Accounting Office, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, GAO-02-474 (Washington, D.C.: July 15, 2002).

[5] U.S. General Accounting Office, *Aviation Security: Transportation Security Administration Faces Immediate and Long-Term Challenges*, GAO-02-971T (Washington, D.C.: July 25, 2002).

[6] U.S. General Accounting Office, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters Is Limited*, GAO-01-780 (Washington, D.C.: July 2001).

Technological Impediments

This country has tremendous resources at its disposal, including leading edge technologies, a superior research and development base, extensive expertise, and significant human capital resources.[7] However, there are substantial challenges in leveraging these tools and using them effectively to ensure that timely, useful information is appropriately disseminated to prevent or minimize terrorist attacks. One challenge is determining and implementing the right format and standards for collecting data so that disparate agencies can aggregate and integrate data sets. For example, Extensible Markup Language (XML) standards are one option for exchanging information among disparate systems.[8] Further, guidelines and procedures need to be specified to establish effective data collection processes, and mechanisms need to be put in place to make sure that this happens – again, a difficult task, given the large number of government, private, and other organizations that will be involved in data collection. Mechanisms will be needed to disseminate data, making sure that it gets into the hands of the right people at the right time. It will be equally important to disaggregate information in order to build baselines (normative models) of activity for detecting anomalies that would indicate the nature and seriousness of particular vulnerabilities. Additionally, there is a lack of connectivity between databases and technologies important to the homeland security effort. Databases belonging to federal law enforcements agencies, for example, are frequently not connected, nor are the databases of the federal, state, and local governments. In fact, we have reported for years on federal information systems that are duplicative and not well integrated.[9]

[7]U.S. General Accounting Office, *National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy*, GAO-02-811T (Washington, D.C.: June 7, 2002).

[8]XML is the universal format for structured documents and data on the Web that makes it easy for a computer to generate data, read data, and ensure that the data structure is unambiguous. XML avoids common pitfalls in language design: It is extensible, platform-independent, and supports internationalization and localization. XML is a flexible, nonproprietary set of standards for annotating or "tagging" information so that it can be transmitted over a network and readily interpreted by disparate systems. For more information on its potential use for electronic government initiatives, see U.S. General Accounting Office, *Electronic Government: Challenges to Effective Adoption of the Extensible Markup Language*, GAO-02-327 (Washington, D.C.: April 2002).

[9]U.S. General Accounting Office, *Information Technology: Enterprise Architecture Use Across the Federal Government Can Be Improved*, GAO-02-6 (Washington, D.C.: February 2002).

Ineffective Collaboration

Ineffective collaboration among homeland security stakeholders remains one of the principal impediments to integrating and sharing information in order to prevent and minimize terrorist attacks. The committees' joint inquiry staff's initial report detailing numerous examples of strategic information known by the intelligence community prior to September 11th highlights the need to better ensure effective integration, collaboration, and dissemination of critical material.[10] The joint inquiry staff's report focuses on the national intelligence community, but its implications are clearly evident for all homeland security stakeholders – government at all levels, as well as the private sector, must work closely together to analyze, integrate, and appropriately disseminate all useful information to the relevant stakeholders in order to combat terrorism and make the nation more secure.

GAO recognizes that this goal is easier to articulate than achieve and that some long-standing obstacles to improving information sharing between and among stakeholders at all levels will require significant changes in organizational cultures, shifts in patterns of access to and limitations on information, and improved processes to facilitate communication and interaction.

GAO's ongoing work illuminates some of the issues. For instance, officials from the Department of Justice, FBI, and the Office of the Secretary of Defense indicated that the vast majority of information—about 90 percent—is already publicly available, and that only about 10 percent of the information is classified, sensitive, or otherwise restricted. The officials said that the expectation for all homeland security participants to obtain actionable information (actionable intelligence is information that is specific enough to tell who, what, where, and when an attack will take place) is unrealistic because, in most cases, the data do not exist or cannot be recognized as actionable. These officials also said that they do share actionable information with appropriate entities, but must also balance the release of the information against the possibility of disclosures that may reveal the sources and methods used to collect the information.

Non federal officials tend to echo these concerns. Since September 11th, GAO has met with representatives of various state and local organizations

[10]U.S. Congress, House and Senate Select Intelligence Committees, *Joint Inquiry Staff Statement, Part I*, (Washington, D.C.: September 18, 2002).

and conducted dozens of case studies of transit authorities, port authorities, and pipeline safety commissions and others entities, as well as testified before and heard testimonies from federal, state, and local officials at 11 congressional field hearings around the country. State and local officials continue to be frustrated by difficulties in the communication and sharing of threat information among all levels of government. Some of the problems they cited include: limited access to information because of security clearance issues, the absence of a systematic top-down and bottom-up information exchange, and uncertainties regarding the appropriate response to a heightened alert from the new homeland security advisory system. It is clear that sharing, analyzing, integrating, and disseminating information needs to occur both in and between all levels of government – and throughout organizations both vertically and horizontally.

A number of steps have been taken to address these issues, but clearly more needs to be done. Following the terrorist attacks of September 11th, a review by the Department of Justice found that America's ability to detect and prevent terrorism has been undermined significantly by restrictions that limit the intelligence and law enforcement communities' access to, and sharing of, information. The USA Patriot Act, enacted shortly after the terrorist attacks, was designed to address this problem through enhanced information sharing and updating information-gathering tools. The Patriot Act gives federal law enforcement agencies greater freedom to share information and to coordinate their efforts in the war on terrorism. Methods to use this authority are now being established and implemented, but the effectiveness of these changes will need to be evaluated.

Moreover, the private sector has a critical role in reducing our vulnerability from terrorists. The national strategy for homeland security states: "Government at the federal, state, and local level must actively collaborate and partner with the private sector, which controls 85 percent of America's infrastructure."[11] The strategy further states that the government at all levels must enable the private sector's ability to carry out its protection responsibilities through effective partnerships and designates the proposed DHS as the primary contact for coordination at the federal level.

[11]The White House, *The National Strategy for Homeland Security* (Washington, DC, July 16, 2002).

Recently, the President's Critical Infrastructure Protection Board issued a strategy recognizing that all Americans have a role to play in cyber security, and identifies the market mechanisms for stimulating sustained actions to secure cyberspace.[12] The strategy recommends that the federal government identify and remove barriers to public-private information sharing and promote the timely two-way exchange of data to promote increased cyberspace security. Although industry groups already exchange security data, confidentiality concerns over the release of information may limit private sector participation. For example, the technology industry has said that any security information shared with the government should be exempt from disclosure under the Freedom of Information Act, which provides that any person has the right to request access to federal agency records or information.

GAO has also reported on how public-private information sharing practices can benefit CIP. In a report issued last October, GAO cited a number of important practices, including:

- establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;
- developing standards and agreements on how information will be used and protected;
- establishing effective and appropriately secure communications mechanisms; and
- taking steps to ensure that sensitive information is not inappropriately disseminated, which may require statutory change.[13]

Clearly, these practices are applicable to intelligence and information sharing in the broadest sense—and for stakeholders. Effectively implementing these practices will require using the full range of management and policy tools.

[12] The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace*, Draft (Washington, D.C.: September 2002).

[13] U.S. General Accounting Office, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection* GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

Addressing the Challenges

GAO believes that the challenges facing the homeland security community require a commitment to focus on transformational strategies, including strengthening the risk management framework, refining the strategic and policy guidance structure to emphasize collaboration and integration among all relevant stakeholders, and bolstering the fundamental management foundation integral to effective public sector performance and accountability. Implementation of these strategies along with effective oversight will be necessary to institutionalize and integrate a long-term approach to sustainable and affordable homeland security.

Comprehensive Risk and Threat Assessment Needed

The events of September 11th have clearly shown the need for a comprehensive risk and threat assessment. Such an assessment, which needs to be integrated at all levels within the homeland security community, is necessary to better protect the nation's people, borders, and property. As your committees' work indicates, threats are many, and sources are numerous.

A comprehensive assessment can help the nation to better understand and manage the risks associated with terrorism. Moreover, a comprehensive risk and threat assessment is critical to setting priorities and allocating resources. There is no such thing as zero risk and, therefore, hard choices must be made given our limited resources over the coming years.

Previously, GAO observed that the federal government has not effectively planned and implemented risk assessment and management efforts. We noted in testimony before Congress last October that individual federal agencies have efforts under way, but the results to date have been inconclusive.[14] In the past, we have recommended that the FBI and the DOD enhance their efforts to complete threat and vulnerability assessments and to work with state and local governments in order to provide comprehensive approaches. Although some of this work was accomplished, delays resulting from the September 11th attacks have prevented their completion. Nevertheless, assessments can help in efforts to pinpoint risks and reallocate resources: For example, after September 11th the Coast Guard conducted initial risk assessments of the nation's ports. The Coast Guard identified high-risk infrastructure and facilities

[14]U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: October 31, 2001).

within specific areas of operation, which helped it to determine how to deploy resources to better ensure harbor security.

The Administration clearly recognizes the importance of such assessments. The national homeland security strategy points out that vulnerability assessments must be an integral part of the intelligence cycle for homeland security activities. They would allow planners to project the consequences of possible terrorist attacks against specific facilities or different sectors of the economy or government. The strategy also states the U.S. government does not now perform comprehensive vulnerability assessments of all the nation's critical infrastructure and key assets.

Integration of Strategic and Policy Framework Needed

GAO has long advocated the development and implementation of a national strategy to integrate and manage homeland security functions. The national strategy for homeland security released by the Administration last summer recognizes information sharing and systems as key factors cutting across all mission areas in linking and more effectively using the nation's information systems to better support homeland security. The issuance of this strategy is a very important step. Moreover, information systems and processes will need to be better integrated to support the goals established by the strategy.

In our current world, we can no longer think of information sharing, analysis, integration, and dissemination in terms of just the traditional intelligence community. Today, a broader network for information sharing includes the traditional intelligence community, U.S. allies, other federal agencies, state and local governments, and the private sector. To optimize such a network, it is important to have a strong, strategic planning framework and a supporting policy structure.

In addition, the national strategy identified one key homeland security mission area as intelligence and warning to detect and prevent terrorist actions. The intent is to provide timely and useful actionable information based on the review and analysis of homeland security information. The national strategy describes a number of initiatives to better develop opportunities for leveraging information sharing among homeland security stakeholders, including:

- Integrate information sharing across the federal government. This initiative addresses coordinating the sharing of essential homeland security information, including the design and implementation of an

interagency information architecture to support efforts to find, track, and respond to terrorist threats. This effort is among the Administration's budget priorities for fiscal year 2004.

- Integrate information sharing across state and local governments, private industry, and citizens. This initiative describes efforts to disseminate information from the federal government to state and local homeland security officials. One effort, to allow the exchange of information on federal and state government Web sites, has been completed.

- Adopt common "meta-data" standards for electronic information relevant to homeland security. This initiative is intended to integrate terrorist-related information from government databases and allow the use of "data mining" tools for homeland security. This effort is under way.

- Improve public safety emergency communications. This initiative is intended to develop comprehensive emergency communications systems that can disseminate information about vulnerabilities and protective measures and help manage incidents. State and local governments often report that there are deficiencies in their communications capabilities, including the lack of interoperable systems. Such systems are necessary between and among all levels of government. This effort is planned, but no timeline is indicated.

- Ensure reliable public health information. The last initiative is intended to address reliable communication between medical, veterinary, and public health organizations. It is under way.

While these initiatives provide a starting point for improved information sharing, their effective and timely implementation is not assured. A commitment to achieve these objectives must be emphasized. Implementation will require integration, coordination, and collaboration between organizations both within and outside the federal government. Further, the initiatives tend to rely on the creation of DHS for their complete implementation, a department that will require a considerable transition period to reach full potential. Improvements in efficiency and effectiveness are expected in the long term, but there will be additional costs and challenges, as the new department faces tremendous communications, human capital, information technology, and other integration, challenges.[15]

Moreover, it is also important to note that the national strategy for homeland security is one of several national strategies that address general and specific security and terrorism related issues. In addition to the homeland security strategy, the Administration recently released a national security strategy. The Administration has stated that the national security strategy could, in conjunction with the homeland security strategy, be viewed as an overarching framework. There are also requirements for several other strategies that cover specific aspects of national and homeland security. These include the National Strategy for Combating Terrorism, National Strategy to Combat Weapons of Mass Destruction, National Strategy to Secure Cyberspace, National Money Laundering Strategy, National Defense Strategy, and National Drug Control Strategy. These strategies reflect important elements supporting national and homeland security.

In is important that clear linkages be established among the various strategies to ensure common purpose within an overarching framework in order to clearly define specific roles, responsibilities, and resource priorities. An overarching, integrated framework can help to sort out issues of potential duplication, overlap, and conflict – not only for the federal government, but for all key stakeholders. While the individual plans will articulate roles and responsibilities, as well as set goals, objectives and priorities for their areas, effective integration is necessary to ensure that initiatives are undertaken that complement, not conflict with, each other.

[15]U.S. General Accounting Office, *Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will be Pivotal to Success*, GAO-02-886T (Washington, D.C.: June 25, 2002).

Further, integration would allow for the better utilization of resources. Given the many challenges we face, we do not have the resources do everything and must make some hard choices.

Finally, a comprehensive, integrated strategic framework requires a review of the policies and processes that currently guide sharing, analysis, integration, and dissemination of intelligence and other critical information to homeland security stakeholders. Indeed, the policy structure currently in place is principally the product of a Cold War environment, in which threats to the United States occurred mainly on foreign soil. New and emerging threats clearly demonstrate that terrorist acts can – and will – impact America at home. The changing nature of the threats present an opportunity for the homeland security community to revisit the legal and policy structure to ensure that it effectively creates an environment for the type of broad-based information sharing needed to protect America at home. It is not just the intelligence community, or the federal government, that have roles, as well as needs, in this evolving environment. Information can be collected by many sources and analyzed to identify potential threats. This information must be disseminated to all relevant parties – whether it is to a federal agency or another level of government. The volume and sonrces of threats, as your committees have reported, present new and serious challenges to our ability to analyze and integrate information into meaningful threat assessments. Not least, this will require attention to government's capacity to handle the increased volume of information.

Our policy structures need to adapt to these challenges. In fact, the government has recently implemented several measures that promote the sharing of information between all levels of government. For example, the USA Patriot Act provides for greater sharing of intelligence information among federal agencies. The FBI has also implemented several initiatives that would increase information sharing between all levels of government, including increasing the number of its Joint Terrorism Task Forces, to be located at each of its 56 field offices; and establishing the Terrorism Watch List to serve as its single, integrated list of individuals of investigative interest. The FBI plans to make the list accessible throughout the law enforcement and intelligence communities.

All of these are recent changes, of course, and will take time to fully implement. It will be important to assess how effective these and other changes are in promoting needed and appropriate information sharing. GAO stands ready to assist the Congress in these efforts.

Management Success Factors

As the recent proposals to create DHS indicate, the terrorist events of last fall have provided an impetus for the government to look at the larger picture of how it provides homeland security and how it can best accomplish associated missions – both now and over the long term. This imperative is particularly clear for the homeland security community, where information sharing and collaboration issues remain a challenge. In this environment, there exists a very real need and possibly a unique opportunity to rethink approaches and priorities to enable the homeland security community to better target its resources to address the most urgent needs. In some cases, the new emphasis on homeland security has prompted attention to long-standing problems that have suddenly become more pressing. In other cases, it will be equally important for organizations to focus on the fundamental building blocks necessary for effective public sector performance and accountability – foundations that readily apply to the homeland security community.

In recent months, we have testified about the long-term implementation challenges that the homeland security community faces – not only in ensuring an effective transition to a consolidated DHS, but in strengthening the relationships among and between all stakeholders to facilitate transformational change that can be sustained in years to come. There are many tools that organizations involved in homeland security might consider to drive necessary changes for better collaboration and integration of information sharing activities. One such tool is the Chief Operating Officer (COO) concept. Strategic positioning of COOs can provide a central point to elevate attention on management issues and transformational change, to integrate various key management functions and responsibilities, and to institutionalize accountability for management issues and leading change.

Despite some assertions to the contrary, there is no meaningful distinction between the intelligence community, other homeland security organizations, or even other public sector agencies when it comes to creating an environment where strong leadership and accountability for results drives a transformational culture. Over the years, GAO has made observations and recommendations about many success factors required for public sector effectiveness, based on effective management of people, technology, financial, and other issues, especially in its biannual Performance and Accountability Series on major government departments.[15] These factors include the following:

- Strategic Planning: Leading results-oriented organizations focus on the process of strategic planning that includes involvement of stakeholders, assessment of internal and external environments, and an alignment of activities, core processes and resources to support mission-related outcomes.

- Organizational Alignment: Operations should be aligned in a way that provides for effective sharing of information, consistent with the goals and objectives established in the national homeland security strategy.

- Communication: Effective communication strategies are key to any major transformation effort and help to instill an organizational culture that lends itself to effective sharing of information.

- Building Partnerships: A key challenge is the development and maintenance of homeland security partners at all levels of the government and the private sector, both in the United States and overseas.

- Performance Management: An effective performance management system fosters institutional, unit, and individual accountability.

- Human Capital Strategy: As with other parts of the government, homeland security agencies must ensure that their homeland security missions are not adversely impacted by the government's pending human capital crisis, and that they can recruit, retain, and reward a

[15] U.S. General Accounting Office, *Major Management Challenges and Program Risks: A Governmentwide Perspective*, GAO-01 241 (Washington, D.C.: January 2001).

talented and motivated workforce, which has required core competencies, to achieve their mission and objectives.

- Information Management and Technology: State-of-the art enabling technology is critical to enhance the ability to transform capabilities and capacities to share and act upon timely, quality information about terrorist threats.

- Knowledge Management: The homeland security community must foster policies and activities that make maximum use of the collective body of knowledge that will be brought together to determine and deter terrorist threats.

- Financial Management: All public sector entities have a stewardship obligation to prevent fraud, waste and abuse, to use tax dollars appropriately, and to ensure financial accountability to the President, Congress and the American people.

- Acquisition Management: The homeland security community, along with the proposed DHS, in the coming years will potentially have one of the most extensive acquisition requirements in government. High-level attention to strong systems and controls for acquisition and related business processes will be critical both to ensuring success and maintaining integrity and accountability.

- Risk Management: Homeland security agencies must be able to maintain and enhance current states of readiness while transitioning and transforming themselves into more effective and efficient collaborative cultures.

Creating and sustaining effective homeland security organizations will require strong commitment to these public sector foundations to foster our nation's safety.

Building Effective Systems

Of all the management success factors applicable to the homeland security community, one of the most important is the establishment of effective communications and information systems. Such systems will likely be critical to our efforts to build an integrated approach to information sharing. Meaningful understanding of inter- and intra-agency information sharing (intelligence or otherwise) necessitates the development of models depicting both how this occurs today and how this should occur tomorrow

to optimize mission performance. Such modeling is referred to as developing and implementing enterprise architectures, which in the simplest of terms can be described as blueprints (both business and technology) for transforming how an organization operates. Included in these architectures are information models defining, among other things, what information is needed and used by whom, where, when, and in what form. Without having such an architectural context within which to view the entity in question, a meaningful understanding of the strengths and weaknesses of information sharing is virtually impossible.

Currently, such an understanding within the homeland security arena does not exist. At OHS steps are being taken to develop enterprise architectures for each of the proposed department's four primary mission areas. According to the chief architect for this effort, working groups have been established for three of the four homeland security mission areas and they are in the process of developing business models (to include information exchange matrixes), that are based on the national strategy and that define how agencies currently perform these mission areas. For the fourth, which is information analysis and infrastructure protection (i.e., intelligence information sharing), the office is in the process of forming the working group. The goal of the groups is to follow OMB's enterprise architecture framework,[17] and deliver an initial set of architecture models describing how homeland security agencies operate by December 31, 2002.

Human Capital Emphasis

Human capital is another critical ingredient required for homeland security success. The government-wide increase in homeland security activities has created a demand for personnel with skills in areas such as information technology, foreign language proficiencies, and law enforcement – without whom, critical information has less chance of being shared, analyzed, integrated, and disseminated in a timely, effective manner. A GAO report issued in January 2002 stresses that foreign language translator shortages, combined in part with advances in technology, at some federal agencies have exacerbated translation backlogs in intelligence and other information. These shortfalls have adversely affected agency operations

[17]This framework provides for the following set of reference models: business, performance measures, data and information, application capabilities, and technology and standards.

and hindered U.S. military, law enforcement, intelligence, counter terrorism and diplomatic efforts.[18]

GAO believes it is reasonable for certain human capital and management flexibilities to be granted, provided that they are accompanied by adequate transparency and appropriate safeguards designed to prevent abuse and to provide for Congressional oversight. Such flexibilities might prove useful to other entities involved in critical information sharing activities. Moreover, the proposed department, similar to other federal agencies, would benefit from integrating a human capital strategy within its strategic planning framework. Naturally, this framework would apply to the intelligence community at large, as well as other homeland security stakeholders.

While recent events certainly underscore the need to address the federal government's human capital challenges, the underlying problem emanates from the longstanding lack of a consistent strategic approach to marshaling, managing, and maintaining the human capital needed to maximize government performance and assure government's accountability. Serious human capital shortfalls are eroding the capacity of many agencies, and threatening the ability of others to economically, efficiently, and effectively perform their missions. The federal government's human capital weaknesses did not emerge overnight and will not be quickly or easily addressed. Committed, sustained, and inspired leadership and persistent attention from all interested parties will be essential if lasting changes are to be made and the challenges we face successfully addressed.

GAO's model of strategic human capital management embodies an approach that is fact-based, focused on strategic results, and incorporates merit principles and other national goals. As such, the model reflects two principles central to the human capital idea:

- People are assets whose value can be enhanced through investment. As with any investment, the goal is to maximize value while managing risk.
- An organization's human capital approaches should be designed, implemented, and assessed by the standard of how well they help the

[18]U.S. General Accounting Office, *Foreign Languages: Human Capital Approach Needed to Correct Staffing and Proficiency Shortfalls*, GAO-02-375 (Washington, D.C.: January 2002).

organization pursue its mission and achieve desired results or outcomes.

The cornerstones to effective human capital planning include leadership; strategic human capital planning; acquiring, developing and retaining talent; and building results-oriented organizational cultures. The homeland security and intelligence communities must include these factors in their management approach in order to leverage high performance organizations in this critical time.

Institutional Oversight

Finally, it is important to note that the success of our nation's efforts to defend and protect our homeland against terrorism depends on effective oversight by the appropriate parts of our government. The oversight entities of the executive branch – including the Inspectors General, the OMB and OHS – have a vital role to play in ensuring expected performance and accountability. Likewise, the committees of the Congress and the GAO, as the investigative arm of the legislative branch, have long term and broad institutional roles to play in supporting the nation's efforts to strengthen homeland security and prevent and mitigate terrorism. GAO recognizes the sensitive issues surrounding oversight of the intelligence and law enforcement communities, and we work collaboratively to find a balance between facilitating the needs of legitimate legislative oversight and preventing disclosure of national security and law enforcement sensitive information. Yet, as GAO has testified previously, our ability to be fully effective in our oversight role of homeland security, including the intelligence community, is at times limited. Historically, the FBI, CIA, NSA, and others have limited our access to information, and Congress's request for evaluations of the CIA have been minimal.[19] Given both the increasing importance of information sharing in preventing terrorism and the increased investment of resources to strengthen homeland security, it seems prudent that constructive oversight of critical intelligence and information sharing operations by the legislative branch be focused on the implementation of a long term transformation program and to foster information sharing in the homeland security community.

[19]U.S. General Accounting Office, *Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities*, GAO-01-975T (Washington, D.C.: July 18, 2001).

In summary, I have discussed the challenges and approaches to improving information sharing among homeland security organizations, as well as the overall management issues that they face along with other public sector organizations. However, the single most important element of any successful transformation is the commitment of top leaders. Top leadership involvement and clear lines of accountability for making management improvements are critical to overcoming an organization's natural resistance to change, marshaling the resources needed to improve management, and building and maintaining organization-wide commitment to new ways of doing business. Organizational cultures will not be transformed, and new visions and ways of doing business will not take root without strong and sustained leadership. Strong and visionary leadership will be vital to creating a unified, focused homeland security community whose participants can act together to help protect our homeland.

This concludes my written testimony. I would be pleased to respond to any questions that you or members of the committees may have.

Appendix I

GAO Recommendations on Combating Terrorism and Homeland Security

This appendix provides a compendium of selected GAO recommendations for combating terrorism and homeland security and their status. GAO has conducted a body of work on combating terrorism since 1996 and, more recently, on homeland security. Many of our recommendations have been either completely or partially implemented, with particular success in the areas of (1) defining homeland security, (2) developing a national strategy for homeland security, (3) creating a central focal point for coordinating efforts across agencies, (4) tracking funds to combat terrorism, (5) improving command and control structures, (6) developing interagency guidance, (7) improving the interagency exercise program to maintain readiness, (8) tracking lessons learned to improve operations, (9) protecting critical infrastructure, (10) protecting military forces, (11) consolidating first responder training programs, (12) managing materials used for weapons of mass destruction, and (13) improving coordination of research and development. Overall, federal agencies have made realistic progress in many areas given the complexity of the environment confronting them. Many additional challenges remain, however, and some of GAO's previous recommendations remain either partially implemented or have not been implemented at all.

The information below details many of our key recommendations and the status of their implementation. The implementation of many of these recommendations may be affected by current proposals to transfer certain functions from a variety of federal agencies to the proposed Department of Homeland Security. Some of the recommendations have been modified slightly to fit into this format.

Combating Terrorism: Status of DOD Efforts to Protect Its Forces Overseas (GAO/NSIAD-97-207, July 21, 1997). Recommendations, p. 20.

GAO recommendations	Status of recommendations
We recommend that the Secretary of Defense direct the Chairman of the Joint Chiefs of Staff to develop common standards and procedures to include (1) standardized vulnerability assessments to ensure a consistent level of quality and to provide a capability to compare the results from different sites, (2) Department of Defense (DOD)-wide physical security standards that are measurable yet provide a means for deviations when required by local circumstances, and (3) procedures to maintain greater consistency among commands in their implementation of threat condition security measures.	Implemented. (1) The Joint Staff has sponsored hundreds of vulnerability assessments—known as Joint Staff Integrated Vulnerability Assessments—based on a defined set of criteria. (2) The Joint Staff has issued one volume of DOD-wide construction standards in December 1999, and plans to complete two additional volumes by December 2002. (3) DOD has provided more guidance and outreach programs to share lessons learned among commands.
To ensure that security responsibility for DOD personnel overseas is clear, we recommend that the Secretary of Defense take the necessary steps to ensure that the memorandum of understanding now under discussion with the Department of State is signed expeditiously. Further, the Secretary should provide the geographic combatant commanders with the guidance to successfully negotiate implementation agreements with chiefs of mission.	Implemented. The Departments of Defense and State have signed a memorandum of understanding, and scores of country-level memorandums of agreement have been signed between the geographic combatant commanders and their local U.S. ambassadors or chiefs of mission. These agreements clarify who is responsible for providing antiterrorism and force protection to DOD personnel not under the direct command of the geographic combatant commanders.

Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination (GAO/NSIAD-98-39, Dec. 1, 1997). Recommendations, p. 13.

GAO recommendations	Status of recommendations
We recommend that consistent with the responsibility for coordinating efforts to combat terrorism, the Assistant to the President for National Security Affairs of the National Security Council (NSC), in consultation with the Director, Office of Management and Budget (OMB), and the heads of other executive branch agencies, take steps to ensure that (1) governmentwide priorities to implement the national counterterrorism policy and strategy are established, (2) agencies' programs, projects, activities, and requirements for combating terrorism are analyzed in relation to established governmentwide priorities, and (3) resources are allocated based on the established priorities and assessments of the threat and risk of terrorist attack.	Partially implemented. (1) The Attorney General's Five-Year Counter-Terrorism and Technology Crime Plan, issued in December 1998, included priority actions for combating terrorism. According to NSC and OMB, the Five-Year Plan, in combination with Presidential Decision Directives (PDD) 39 and 62, represented governmentwide priorities that they used in developing budgets to combat terrorism. (2) According to NSC and OMB, they analyzed agencies' programs, projects, activities, and requirements using the Five-Year Plan and related presidential decision directives. (3) According to NSC and OMB, they allocated agency resources based upon the priorities established above. More recently, the Office of Homeland Security issued a National Strategy for Homeland Security, which also established priorities for combating terrorism domestically. However, there is no clear link between resources and threats because no national-level risk management approach has been completed to use for resource decisions.
To ensure that federal expenditures for terrorism-related activities are well-coordinated and focused on efficiently meeting the goals of U.S. policy under PDD 39, we recommend that the Director, OMB, use data on funds budgeted and spent by executive departments and agencies to evaluate and coordinate projects and recommend resource allocation annually on a crosscutting basis to ensure that governmentwide priorities for combating terrorism are met and programs are based on analytically sound threat and risk assessments and avoid unnecessary duplication.	Partially implemented. OMB now is tracking agency budgets and spending to combat terrorism. According to NSC and OMB, they have a process in place to analyze these budgets and allocate resources based upon established priorities. More recently, OMB also started tracking spending on homeland security—the domestic component of combating terrorism. However, there is no clear link between resources and threats. No national-level risk management approach has been completed to use for resource decisions.

Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency (GAO/NSIAD-99-3, Nov. 12, 1998). Recommendations, p. 22.

GAO recommendations	Status of recommendations
We recommend that the Secretary of Defense—or the head of any subsequent lead agency—in consultation with the other five cooperating agencies in the Domestic Preparedness Program, refocus the program to more efficiently and economically deliver training to local communities.	Implemented. DOD transferred the Domestic Preparedness Program to the Department of Justice on October 1, 2000. The Department of Justice implemented this recommendation by emphasizing the program's train-the-trainer approach and concentrating resources on training metropolitan trainers in recipient jurisdictions. In June 2002, the President proposed that a new Department of Homeland Security take the lead for federal programs to assist state and local governments.
We recommend that the Secretary of Defense, or the head of any subsequent lead agency, use existing state and local emergency management response systems or arrangements to select locations and training structures to deliver courses and consider the geographical proximity of program cities.	Implemented. DOD transferred the Domestic Preparedness Program to the Department of Justice on October 1, 2000. The Department of Justice implemented this recommendation by modifying the programs in metropolitan areas and requiring cities to include their mutual aid partners in all training and exercise activities. In June 2002, the President proposed that a new Department of Homeland Security take the lead for federal programs to assist state and local governments.
We recommend that the National Coordinator for Security, Infrastructure Protection and Counterterrorism actively review and guide the growing number of weapons of mass destruction (WMD) consequence management training and equipment programs and response elements to ensure that agencies' separate efforts leverage existing state and local emergency management systems and are coordinated, unduplicated, and focused toward achieving a clearly defined end state.	Partially implemented. NSC established an interagency working group called the Interagency Working Group on Assistance to State and Local Authorities. One function of this working group was to review and guide the growing number of WMD consequence management training and equipment programs. In a September 2002 report, we reported that more needs to be done to ensure that federal efforts are coordinated, unduplicated, and focused toward achieving a clearly defined end state—a results-oriented outcome as intended for government programs by the Results Act. In June 2002, the President proposed that a new Department of Homeland Security take the lead for federal programs to assist state and local governments.

Combating Terrorism: Issues to Be Resolved to Improve Counterterrorism Operations (GAO/NSIAD-99-135, May 13, 1999).

GAO recommendations	Status of recommendations
We recommend that the Attorney General direct the Director, Federal Bureau of Investigation (FBI), to coordinate the Domestic Guidelines and concepts of operation plan (CONPLAN) with federal agencies with counterterrorism roles and finalize them. Further, the Domestic Guidelines and/or CONPLAN should seek to clarify federal, state, and local roles, missions, and responsibilities at the incident site.	Implemented. The Domestic Guidelines were issued in November 2000. The CONPLAN was coordinated with key federal agencies and was issued in January 2001.
We recommend that the Secretary of Defense review command and control structures, and make changes, as appropriate, to ensure there is unity of command to DOD units participating in domestic counterterrorist operations to include both crisis response and consequence management and cases in which they might be concurrent.	Implemented. In May 2001, the Secretary of Defense assigned responsibility for providing civilian oversight of all DOD activities to combat terrorism and domestic WMD (including both crisis and consequence management) to the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. Further, in October 2002, DOD will establish a new military command—the Northern Command—to manage command and control in domestic military operations to combat terrorism in support of other federal agencies.
We recommend that the Secretary of Defense require the services to produce after-action reports or similar evaluations for all counterterrorism field exercises that they participate in. When appropriate, these after-action reports or evaluations should include a discussion of interagency issues and be disseminated to relevant internal and external organizations.	Partially implemented. DOD has used its Joint Uniform Lessons Learned System to document observations and lessons learned during exercises, including interagency counterterrorist exercises. Many DOD units produce after-action reports and many of them address interagency issues. However, DOD officials acknowledged that service units or commands do not always produce after-action reports and/or disseminate them internally and externally as appropriate.

Combating Terrorism: Use of National Guard Response Teams Is Unclear (GAO/NSIAD-99-110, May 21, 1999). Recommendations, p. 20.

GAO recommendations	Status of recommendations
We recommend that the National Coordinator for Security, Infrastructure Protection and Counterterrorism, in consultation with the Attorney General, the Director, Federal Emergency Management Agency (FEMA), and the Secretary of Defense, reassess the need for the Rapid Assessment and Initial Detection teams in light of the numerous local, state, and federal organizations that can provide similar functions and submit the results of the reassessment to Congress. If the teams are needed, we recommend that the National Coordinator direct a test of the Rapid Assessment and Initial Deployment team concept in the initial 10 states to determine how the teams can best fit into coordinated state and federal response plans and whether the teams can effectively perform their functions. If the teams are not needed, we further recommend that they be inactivated.	Partially implemented. With authorization from Congress, DOD established additional National Guard teams and changed their names from Rapid Assessment and Initial Detection teams to WMD Civil Support Teams. However, subsequent to our report and a report by the DOD Inspector General, which found some similar problems, DOD agreed to review the National Guard teams and work with other agencies to clarify their roles in responding to terrorist incidents. In September 2001, DOD restricted the number of teams to 32.

Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attack (GAO/NSIAD-99-163, Sept. 7, 1999). Recommendations, p. 22.

GAO recommendations	Status of recommendations
We recommend that the Attorney General direct the FBI Director to prepare a formal, authoritative intelligence threat assessment that specifically assesses the chemical and biological agents that would more likely be used by a domestic-origin terrorist—nonstate actors working outside a state-run laboratory infrastructure.	Partially implemented. The FBI agreed with our recommendation. The FBI, working with the National Institute of Justice and the Technical Support Working Group, produced a draft threat assessment of the chemical and biological agents that would more likely be used by terrorists. FBI officials originally estimated it would be published in 2001. However, the terrorist attacks in the fall of 2001 delayed these efforts. The FBI and the Technical Support Working Group are now conducting an updated assessment of chemical and biological terrorist threats. According to the FBI, the assessment is being done by experts in WMD and terrorist training manuals and will include the latest information available. The assessment, once completed, will be disseminated to appropriate agencies.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
We recommend that the Attorney General direct the FBI Director to sponsor a national-level risk assessment that uses national intelligence estimates and inputs from the intelligence community and others to help form the basis for and prioritize programs developed to combat terrorism. Because threats are dynamic, the Director should determine when the completed national-level risk assessment should be updated.	Partially implemented. The Department of Justice and the FBI agreed to our recommendation. According to the FBI, it is currently working on a comprehensive national-level assessment of the terrorist threat to the U.S. homeland. The FBI said that this will include an evaluation of the chemical and biological weapons most likely to be used by terrorists and a comprehensive analysis of the risks that terrorist would use WMD. The FBI estimates the assessment will be completed in November 2002.

Combating Terrorism: Chemical and Biological Medical Supplies Are Poorly Managed (GAO/HEHS/AIMD-00-36, Oct. 29, 1999). Recommendations, p. 10.

GAO recommendations	Status of recommendations
We recommend that the Department of Health and Human Services' (HHS) Office of Emergency Preparedness (OEP) and Centers for Disease Control and Prevention (CDC), the Department of Veterans Affairs (VA), and U.S. Marine Corps Chemical Biological Incident Response Force (CBIRF) establish sufficient systems of internal control over chemical and biological pharmaceutical and medical supplies by (1) conducting risk assessments, (2) arranging for periodic, independent inventories of stockpiles, (3) implementing a tracking system that retains complete documentation for all supplies ordered, received, and destroyed, and (4) rotating stock properly.	Partially implemented. Three of the recommendations have been implemented. However, only VA has implemented a tracking system to manage the OEP inventory. CDC is using an interim inventory tracking system. CBIRF has upgraded its database program to track medical supplies, and is working toward placing its medical supply operations under a prime vendor contract.

Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training (GAO/NSIAD-00-64, Mar. 21, 2000). Recommendations, p. 25.

GAO recommendations	Status of recommendations
We recommend that the Secretary of Defense and the Attorney General eliminate duplicate training to the same metropolitan areas. If the Department of Justice extends the Domestic Preparedness Program to more than the currently planned 120 cities, it should integrate the program with the Metropolitan Firefighters Program to capitalize on the strengths of each program and eliminate duplication and overlap.	Partially implemented. DOD transferred the Domestic Preparedness Program to the Department of Justice on October 1, 2000. The Department of Justice, while attempting to better integrate the assistance programs under its management, continued to run the Domestic Preparedness Program as a separate program. In June 2002, the President proposed that a new Department of Homeland Security take the lead for federal programs to assist state and local governments.

Combating Terrorism: Action Taken but Considerable Risks Remain for Forces Overseas (GAO-00-181, July 19, 2000). Recommendations, p. 26.

GAO recommendations	Status of recommendations
To improve the effectiveness and increase the impact of the vulnerability assessments and the vulnerability assessment reports, we recommend that the Secretary of Defense direct the Chairman of the Joint Chiefs of Staff to improve the vulnerability assessment reports provided to installations. Although the Joint Staff is planning to take some action to improve the value of these reports, we believe the vulnerability assessment reports should recommend specific actions to overcome identified vulnerabilities.	Not implemented. DOD believes that the changes in process at the time of our report addressed our recommendations. DOD is still in the process of implementing these actions.
To ensure that antiterrorism/force protection managers have the knowledge and skills needed to develop and implement effective antiterrorism/force protection programs, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to expeditiously implement the Joint Staff's draft antiterrorism/force protection manager training standard and formulate a timetable for the services to develop and implement a new course that meets the revised standards. Additionally, the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict should review the course content to ensure that the course has consistency of emphasis across the services.	Partially implemented. DOD revised its training standards for antiterrorism/force protection managers, but the Army has not implemented the new training standards.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
We recommend that the Joint Chiefs of Staff should develop an antiterrorism/force protection best practices or lessons learned program that would share recommendations for both physical and process-oriented improvements. The program would assist installations in addressing common problems—particularly those installations that do not receive Joint Staff Integrated Vulnerability Assessment reports or others who have found vulnerabilities through their own assessments.	Partially implemented. The Joint Chiefs of Staff have undertaken a number of lessons learned programs, but not all of the programs that would address this recommendation are operational.
To provide Congress with the most complete information on the risks that U.S. Forces overseas are facing from terrorism, we recommended that the Secretary of Defense direct the services to include in their next consolidated combating terrorism budget submission information on the number and types of antiterrorism/force protection projects that have not been addressed by the budget request and the estimated costs to complete these projects. Information on the backlog of projects should be presented by geographic command.	Not implemented. DOD did not concur with this recommendation. DOD believes that there is no need to provide the additional information to Congress.

Combating Terrorism: Federal Response Teams Provide Varied Capabilities; Opportunities Remain to Improve Coordination (GAO-01-14, Nov. 30, 2000). Recommendations, p. 27.

GAO recommendations	Status of recommendations
To guide resource investments for combating terrorism, we recommend that the Attorney General modify the Attorney General's Five-Year Interagency Counterterrorism and Technology Crime Plan to cite desired outcomes that could be used to develop budget requirements for agencies and their respective response teams. This process should be coordinated as an interagency effort.	Partially implemented. The Department of Justice asserted that the Five-Year Plan included desired outcomes. We disagreed with the department and believed what it cited as outcomes are outputs—agency activities rather than results the federal government is trying to achieve. The National Strategy for Homeland Security, issued in July 2002, supercedes the Attorney General's Five-Year Plan as the interagency plan for combating terrorism domestically. This strategy does not include measurable outcomes, but calls for their development.
We recommend that the Director, FEMA, take steps to require that the WMD Interagency Steering Group develop realistic scenarios involving chemical, biological, radiological, and nuclear agents and weapons with experts in the scientific and intelligence communities.	FEMA agreed with the recommendation. GAO is working with FEMA to determine the status of implementation. In June 2002, the President proposed that a new Department of Homeland Security take the lead for developing and conducting federal exercises to combat terrorism.
We recommend that the Director, FEMA, sponsor periodic national-level consequence management field exercises involving federal, state, and local governments. Such exercises should be conducted together with national-level crisis management field exercises.	FEMA agreed with the recommendation. GAO is working with FEMA to determine the status of implementation. In June 2002, the President proposed that a new Department of Homeland Security take the lead for developing and conducting federal exercises to combat terrorism.

Combating Terrorism: Accountability Over Medical Supplies Needs Further Improvement (GAO-01-463, Mar. 30, 2001). Recommendations, pp. 25 and 26.

GAO recommendations	Status of recommendations
We recommended that the Secretary of HHS require the Director of CDC to • execute written agreements as soon as possible with all CDC's partners covering the storage, management, stock rotation, and transporting of medical supplies designated for treatment of biological or chemical terrorism victims; • issue written guidance on security to private warehouses that store stockpiles; and • to the extent practical, install proper fencing prior to placing inventories at storage locations.	Partially implemented. CDC has implemented two of our recommendations and partially implemented one. Specifically, it has not finalized agreements with private transport companies to transport stockpiles in the event of a terrorist attack. It is currently using contracts between the federal government and the transport companies.
We recommend that the Secretary of HHS require the Director of OEP to • finalize, approve, and issue an inventory requirements list; • improve physical security at its central location to comply with Drug Enforcement Agency regulations, or move the supplies as soon as possible to a location that meets these requirements; • issue a written policy on the frequency of inventory counts and acceptable discrepancy rates; • finalize and implement approved national and local operating plans addressing VA's responsibilities for the procurement, storage, management, and deployment of OEP's stockpiles; • train VA personnel and conduct periodic quality reviews to ensure that national and local operating plans are followed; and • immediately contact Food and Drug Administration or the pharmaceutical and medical supply manufacturers of items stored at its central location to determine the impact of items exposed to extreme temperatures, replace those items deemed no longer usable, and either add environmental controls to the current location or move the supplies as soon as possible to a climate-controlled space.	Implemented. OEP has implemented all eight of our recommendations.
To ensure that medical supplies on hand reflect those identified as being needed to respond to a chemical or biological terrorism incident, we recommend that the Marine Corps Systems Command program funding and complete the fielding plan for the CBIRF specific authorized medical allowance list and that the Commandant of the Marine Corps require the Commanding Officer of CBIRF to adjust its stock levels to conform with the authorized medical allowance list and remove expired items from its stock and replace them with current pharmaceutical and medical supplies.	Implemented. CBIRF has implemented all of our recommendations.

Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities (GAO-01-323, Apr. 25, 2001). Recommendations, pp. 57, 68, and 85.

GAO recommendations	Status of recommendations
We recommend that the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies, • establish a capability for strategic analysis of computer-based threats, including developing a related methodology, acquiring staff expertise, and obtaining infrastructure data; • develop a comprehensive governmentwide data-collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources; and • clearly define the role of the National Infrastructure Protection Center (NIPC) in relation to other government and private-sector entities, including lines of authority among NIPC and NSC, Justice, the FBI, and other entities; NIPC's integration into the national warning system; and protocols that articulate how and under what circumstances NIPC would be placed in a support function to either DOD or the intelligence community.	Partially implemented. According to the NIPC director, NIPC has received sustained leadership commitment from key entities, such as the Central Intelligence Agency and the National Security Agency, and it continues to increase its staff primarily through reservists and contractors. The Director added that the NIPC (1) created an NIPC Senior Partners Group similar to a board of directors, which holds quarterly meetings with the senior leadership of each agency that details personnel to the NIPC in order to ensure that their interests are addressed with respect to future NIPC initiatives and program plans and to share with them the status of ongoing initiatives; (2) has developed close working relationships with other Critical Infrastructure Protection (CIP) entities involved in analysis and warning activities, such as the Federal Computer Incident Response Center (FedCIRC), DOD's Joint Task Force for Computer Network Operations, the Carnegie Mellon CERT® Coordination Center, and the intelligence and antivirus communities, and (3) had developed and implemented procedures to more quickly share relevant CIP information, while separately continuing any related law enforcement investigation. In addition, the Director stated that two additional teams were created to bolster its analytical capabilities: (1) the critical infrastructure assessment team to focus efforts on learning about particular infrastructures and coordinating with respective infrastructure efforts and (2) the collection operations intelligence liaison team to coordinate with various entities within the intelligence community.
We recommend that the Attorney General task the FBI Director to require the NIPC Director to develop a comprehensive written plan for establishing analysis and warning capabilities that integrates existing planning elements and includes • milestones and performance measures; • approaches (or strategies) and the various resources needed to achieve the goals and objectives; • a description of the relationship between the long-term goals and objectives and the annual performance goals; and • a description of how program evaluations could be used to establish or revise strategic goals, along with a schedule for future program evaluations.	Partially implemented. The NIPC Director recently stated that NIPC has developed a plan with goals and objectives to improve its analysis and warning capabilities and that NIPC has made considerable progress in this area. The plan establishes and describes performance measures for both its Analysis and Warning Section and issues relating to staffing, training, investigations, outreach, and warning. In addition, the plan describes the resources needed to reach the specific goals and objectives for the Analysis and Warning Section. According to NIPC officials, the NIPC continues to work on making its goals more measurable, better reflect performance, and better linked to future revisions to strategic goals.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
We recommend that the Attorney General direct the FBI Director to task the NIPC Director to • ensure that the Special Technologies and Applications Unit has access to the computer and communications resources necessary to analyze data associated with the increasing number of complex investigations; • monitor implementation of new performance measures to ensure that they result in field offices' fully reporting information on potential computer crimes to the NIPC; and • complete development of the emergency law enforcement plan, after comments are received from law enforcement sector members.	Partially implemented. According to NIPC officials, the Special Technologies and Applications Unit has continued to increase its computer resources. In addition, the director stated that the NIPC had developed and implemented procedures to more quickly share relevant CIP information, while separately continuing any related law enforcement investigation. However, because of the NIPC's reorganization in August 2002, when the Computer Investigation and Operations Section was moved from NIPC to the FBI's Cyber Crime Division, it is important that NIPC establish procedures to continue this information sharing. In addition, an emergency law enforcement services sector plan has been issued.
As the national strategy for critical infrastructure protection is reviewed and possible changes considered, we recommend that the Assistant to the President for National Security Affairs define NIPC's responsibilities for monitoring reconstitution.	The President's Critical Infrastructure Protection Board released a draft strategy on September 18, 2002, for comment. The draft states that a strategic goal is to provide for a national plan for continuity of operations, recovery, and reconstitution of services during a widespread outage of information technology in multiple sectors. However, NIPC's responsibilities regarding monitoring reconstitution are not discussed.
We recommend that the Assistant to the President for National Security Affairs (1) direct federal agencies and encourage the private sector to better define the types of information that are necessary and appropriate to exchange in order to combat computer-based attacks and procedures for performing such exchanges, (2) initiate development of a strategy for identifying assets of national significance that includes coordinating efforts already under way, such as those at DOD and Commerce, and (3) resolve discrepancies between PDD 63 requirements and guidance provided by the federal Chief Information Officers Council regarding computer incident reporting by federal agencies.	Partially implemented. NIPC officials told us that a new ISAC development and support unit had been created, whose mission is to enhance private-sector cooperation and trust, resulting in a two-way sharing of information. Officials informed us that NIPC has signed information sharing agreements with most of the ISACs formed, including those representing telecommunications, information technology, water supply, food, emergency fire services, banking and finance, and chemical sectors. NIPC officials added that most of these agreements contained industry-specific cyber and physical incident reporting thresholds. NIPC has created the Interagency Coordination Cell to foster cooperation across government agencies in investigative matters and on matters of common interest.
We recommend that the Attorney General direct the FBI Director to direct the NIPC Director to (1) formalize relationships between NIPC and other federal entities, including DOD and the Secret Service, and private-sector Information Sharing Analysis Centers (ISACs) so that a clear understanding of what is expected from the respective organizations exists, (2) develop a plan to foster the two-way exchange of information between the NIPC and the ISACs, and (3) ensure that the Key Asset Initiative is integrated with other similar federal activities.	Partially implemented. According to NIPC's Director, the relationship between NIPC and other government entities has significantly improved since our review, and the quarterly meetings with senior government leaders have been instrumental in improving information sharing. In addition, in testimony, officials from the FedCIRC and the U.S. Secret Service have discussed the collaborative and cooperative relationships that now exist between their agencies and NIPC. However, further work is needed to identify assets of national significance and coordinate with other similar federal activities.

FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters Is Limited (GAO-01-780, July 16, 2001). Recommendations, p. 32.

GAO recommendations	Status of recommendations
To facilitate better coordination of FBI foreign counterintelligence investigations meeting the Attorney General's coordination criteria, we recommend that the Attorney General establish a policy and guidance clarifying his expectations regarding the FBI's notification of the Criminal Division and types of advice that the division should be allowed to provide the FBI in foreign counterintelligence investigations in which the Foreign Intelligence Surveillance Act (FISA) tools are being used or their use is anticipated.	Partially implemented. In an August 6, 2001, memorandum, the Deputy Attorney General outlined the responsibilities of the FBI, Criminal Division, and the Office of Intelligence Policy and Review (OIPR) regarding intelligence sharing in FISA cases and issued clarifications to the Attorney General's 1995 coordination procedures. Specifically, these clarifications included defining "significant federal crime" to mean any federal felony and defining the term "reasonable indication" to be substantially lower than "probable cause." The memorandum also requires notification to take place without delay. The only remaining open point, albeit a significant issue, is the type of advice that the Criminal Division is permitted to provide the FBI after it has been notified of a possible criminal violation. In this regard, in March 2002, the Attorney General signed revised proposed procedures for sharing and coordinating FISA investigations, including changes resulting from the USA Patriot Act of 2001. However, the procedures must be approved by the FISA Court, which recently rejected some of the them as going too far in terms of loosening the barriers between criminal investigations and intelligence gathering.
To improve coordination between the FBI and the Criminal Division by ensuring that investigations that indicate criminal violations are clearly identified and by institutionalizing mechanisms to ensure greater coordination, we recommend that the Attorney General direct that all FBI memorandums sent to OIPR, summarizing investigations or seeking FISA renewals contain a section devoted explicitly to identifying any possible federal criminal violation meeting the Attorney General's coordination criteria, and that those memorandums of investigation meeting the criteria for Criminal Division notification be timely coordinated with the division.	Implemented. In an August 6, 2001, memorandum, the Deputy Attorney General directed the FBI to explicitly devote a section in its foreign counterintelligence case summary memorandums, which it sends to OIPR in connection with an initial FISA request or renewal, for identification of any possible federal criminal violations associated with the cases. OIPR is to make those memorandums available to the Criminal Division. The Deptuy Attorney General's memorandum also required that, when the notification standard is met, notification should be accomplished without delay.
To improve coordination between the FBI and the Criminal Division by ensuring that investigations that indicate a criminal violation are clearly identified and by institutionalizing mechanisms to ensure greater coordination, we recommend that the Attorney General direct the FBI Inspection Division, during its periodic inspections of foreign counterinteligence investigations at field offices, to review compliance with the requirement for case summary memorandums sent OIPR to specifically address the identification of possible criminal violations. Moreover, where field office case summary memorandums identified reportable instances of possible federal crimes, the Inspection Division should assess whether the appropriate headquarters unit properly coordinated those foreign counterintelligence investigations with the Criminal Division.	Implemented. In a July 18, 2001, memorandum to the Deputy Attorney General, the Assistant Director of the FBI's Inspection Division stated that the division has established a Foreign Intelligence/Counterintelligence Audit that is to be completed during its on-site inspections at applicable FBI field offices. The audit, according to the Assistant Director, will determine whether significant criminal activity was indicated during intelligence investigations and, where such activity was identified, determine whether it was properly coordinated with FBI headquarters and Justice's Criminal Division.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
To improve coordination between the FBI and the Criminal Division by ensuring that investigations that indicate criminal violations are clearly identified and by institutionalizing mechanisms to ensure greater coordination, we recommend that the Attorney General issue written policies and procedures establishing the roles and responsibilities of OIPR and the core group as mechanisms for ensuring compliance with the Attorney General's coordination procedures.	Implemented. On June 12, 2001, OIPR issued policy guidance to its staff on compliance with the Attorney General's 1995 coordination procedures. The issuance of this policy partially implements the GAO recommendation. Later on August 6, 2001, the Deputy Attorney General issued a memorandum to the Criminal Division, the FBI and OIPR establishing the roles and responsibilities of the Core Group to resolve disputes arising from the Attorney General's 1995 guidelines.

Combating Terrorism: Actions Needed To Improve DOD Antiterrorism Program Implementation and Management (GAO-01-909, September 19, 2001). Recommendations pp. 26 and 27.

GAO recommendations	Status of recommendations
To improve the implementation of the DOD antiterrorism program, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to identify those installations that serve a critical role in support of our national military strategy, and to ensure that they receive a higher headquarters vulnerability assessment regardless of the number of personnel assigned at the installations.	Partially implemented. DOD is in the process of changing its antiterrorism standards.
To improve the implementation of the DOD antiterrorism program, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to develop a strategy to complete higher headquarters vulnerability assessments at National Guard installations.	Partially implemented. DOD 's primary action officer is working with Army and Air National Guard to provide vulnerability assessments.
To improve the implementation of the DOD antiterrorism program, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to clarify the force protection standard requiring a criticality assessment at each installation to specifically describe the factors to be used in the assessment and how these evaluations should support antiterrorism resource priority decisions.	Partially implemented. DOD is in the process of updating its antiterrorism handbook.
To improve the implementation of the DOD antiterrorism program, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to expand the threat assessment methodology to increase awareness of the consequences of changing business practices at installations that may create workplace violence situations or new opportunities for individuals not affiliated with DOD to gain access to installations.	Implemented. DOD has reviewed its threat methodology to ensure that no threat indicators are ignored or overlooked.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
To improve the implementation of the DOD antiterrorism program, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to require each installation commander to form a threat working group and personally and actively engage state, local, and federal law enforcement officials. These working groups should hold periodic meetings, prepare records of their discussions, and provide threat information to installation commanders regularly.	Partially implemented. DOD is in the process of updating its antiterrorism handbook.
To strengthen management of the antiterrorism program, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to establish a management framework for the antiterrorism program that would provide the department with a vehicle to guide resource allocations and measure the results of improvement efforts. This framework should include A strategic plan that defines • long-term antiterrorism goals, • approaches to achieve the goals, and • key factors that might significantly affect achieving the goals, and An implementation plan that describes • performance goals that are objective, quantifiable, and measurable, and resources to achieve the goals; • performance indicators to measure outputs; • an evaluation plan to compare program results to established goals; and • actions needed to address any unmet goals.	Partially implemented. DOD is planning to issue a management plan to include the elements of GAO's recommendation.

Combating Terrorism: Selected Challenges and Related Recommendations (GAO-01-822, Sept. 20, 2001). Recommendations pp. 41, 42, 57, 86, 87, 104, and 128.

GAO recommendations	Status of recommendations
We recommend that the President, in conjunction with the Vice President's efforts, appoint a single focal point that has the responsibility and authority for all critical leadership and coordination functions to combat terrorism.	Implemented. Through Executive Order (EO) 13228, the President established an Office of Homeland Security (OHS) to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.
• The focal point should be in the Executive Office of the President, outside individual agencies, and encompass activities to include prevention, crisis management, and consequence management.	Implemented. EO 13228 establishes OHS within the Executive Office of the President. OHS functions include efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
• The focal point should oversee a national-level authoritative threat and risk assessment on the potential use of WMD by terrorists on U.S. soil. Such assessments should be updated regularly.	Partially implemented. EO 13228 states that OHS shall identify priorities and coordinate efforts for collection and analysis of information within the United States regarding threats of terrorism against the United States and activities of terrorists or terrorist groups within the United States. OHS shall identify, in coordination with NSC, priorities for collection of intelligence outside the United States regarding threats of terrorism within the United States. EO 13228 does not address risk assessments.
• The focal point also should lead the development of a national strategy for combating terrorism.	Implemented. EO 13228 states that OHS will develop a comprehensive national strategy to secure the United States from terrorist threats or attacks. The National Strategy for Homeland Security was issued in July 2002.
• The national strategy should include (1) desired outcomes that can be measured and are consistent with the Results Act, (2) state and local government input to better define their roles in combating terrorism, and (3) research and development priorities and needs in order to facilitate interagency coordination, decrease duplication, and leverage monetary resources.	Partially implemented. (1) The National Strategy for Homeland Security, while not including measurable outcomes, calls for their development. (2) OHS worked with state and local governments to develop the national strategy. (3) The National Strategy for Homeland Security includes a discussion of research and development.
• The focal point should coordinate implementation of the national strategy among the various federal agencies. This would entail reviewing agency and interagency programs to ensure that they are being implemented in accordance with the national strategy and do not constitute duplication of effort.	Partially implemented. EO 13228 directs OHS to coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. OHS shall work with, among others, federal agencies to ensure the adequacy of the national strategy for detecting, preparing for, preventing, protecting against, responding to, and recovering from terrorist attacks within the United States and shall periodically review and coordinate revisions to that strategy as necessary. The National Strategy for Homeland Security was issued in July 2002. Given the recent publication of the plan, it is too early to determine the OHS role in coordinating its implementation.
• The focal point should analyze and prioritize governmentwide budgets and spending to combat terrorism to eliminate gaps and duplication of effort. The focal point's role will be to provide advice or to certify that the budgets are consistent with the national strategy, not to make final budget decisions.	Implemented. EO 13228 states OHS shall work with OMB and agencies to identify homeland security programs, and shall review and provide advice to OMB and departments and agencies for such programs. Per EO 13228, OHS shall certify that the funding levels are necessary and appropriate for the homeland security-related activities of the executive branch.
• The focal point should coordinate the nation's strategy for combating terrorism with efforts to prevent, detect, and respond to computer-based attacks on critical infrastructures. We do not see the focal point for combating terrorism also having responsibility for protecting computer-based infrastructures because the threats are broader than terrorism and such programs are more closely associated with traditional information security activities. Nonetheless, there should be close coordination between the two areas.	Implemented. Per EO 13228, OHS shall coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. In performing this function, the office shall work with federal, state, and local agencies, and private entities as appropriate to, among other things, coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attacks. In addition, the President created a Special Advisor for Cyberspace Security and appointed him as Chair of the President's Critical Infrastructure Protection Board. This Chair reports to both OHS and NSC.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
• The focal point should be established by legislation to provide it with legitimacy and authority, and its head should be appointed by the President with the advice and consent of the U.S. Senate. This would provide accountability to both the President and Congress. Also, it would provide continuity across administrations.	Not implemented. However, there have been bills before Congress that would legislatively create a central focal point (e.g., OHS), making its director subject to appointment with the advice and consent of the U.S. Senate.
• The focal point should be adequately staffed to carry out its duties for planning and oversight across the federal government.	Partially implemented. EO 13228 has provisions for OHS to hire staff, and for other federal departments to detail their staff to OHS. Given the relative newness of OHS, it is too early to determine whether staff levels are adequate.
• The focal point should develop a formal process to capture and evaluate interagency lessons learned from major interagency and intergovernmental federal exercises to combat terrorism. The focal point should analyze interagency lessons learned and task individual agencies to take corrective actions as appropriate.	Partially implemented. Per EO 13228, OHS shall coordinate domestic exercises and simulations designed to assess and practice systems that would be called upon to respond to a terrorist threat or attack within the United States and coordinate programs and activities for training. OHS shall also ensure that such programs and activities are regularly evaluated under appropriate standards and that resources are allocated to improving and sustaining preparedness based on such evaluations. Given the relative newness of OHS, it is too early to determine how it has implemented this responsibility.
To help support a national strategy, we recommend that the Attorney General direct the Director of the FBI to work with appropriate agencies across government to complete ongoing national-level threat assessments regarding terrorist use of WMD.	Partially implemented. The Department of Justice and the FBI agreed to this recommendation. According to the FBI, it is currently working on a comprehensive national-level assessment of the terrorist threat to the U.S. homeland. The FBI said that this will include an evaluation of the chemical and biological weapons most likely to be used by terrorists and a comprehensive analysis of the risks of terrorists using other WMD. The FBI estimates the assessment will be completed in November 2002.
To guide federal efforts in combating domestic terrorism, we recommend that the Attorney General use the Five-Year Interagency Counterterrorism and Technology Crime Plan and similar plans of other agencies as a basis for developing a national strategy by including (1) desired outcomes that can be measured and that are consistent with the Results Act and (2) state and local government input to better define their roles in combating terrorism.	Partially implemented. The Department of Justice asserted that the Five-Year Plan included desired outcomes. We disagreed with the department and believed what it cited as outcomes are outputs—agency activities rather than results the federal government is trying to achieve. The National Strategy for Homeland Security, issued in July 2002, supercedes the Attorney General's Five-Year Plan as the interagency plan for combating terrorism domestically. This strategy does not include measurable outcomes, but calls for their development.
To improve readiness in consequence management, we recommend that the Director of FEMA play a larger role in managing federal exercises to combat terrorism. As part of this, FEMA should seek a formal role as a cochair of the Interagency Working Group on Exercises and help to plan and conduct major interagency counterterrorist exercises to ensure that consequence management is adequately addressed.	FEMA agreed with the recommendation. GAO is working with FEMA to determine the status of implementation. In June 2002, the President proposed that a new Department of Homeland Security take the lead for developing and conducting federal exercises to combat terrorism.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
To ensure that agencies benefit fully from exercises in which they participate, we recommend that the Secretaries of Agriculture, Defense, Energy, Health and Human Services, and Veterans Affairs; the Directors of the Bureau of Alcohol, Tobacco, and Firearms, FEMA, FBI, and the U.S. Secret Service; the Administrator of the Environmental Protection Agency; and the Commandant of the U.S. Coast Guard require their agencies to prepare after-action reports or similar evaluations for all exercises they lead and for all field exercises in which they participate.	Partially implemented. Several of the agencies agreed with this recommendation and cited steps they were taking to ensure that after-action reports or similar evaluations are completed as appropriate for exercises to combat terrorism. For example, DOD has used its Joint Uniform Lessons Learned System to document observations and lessons learned during exercises, including interagency exercises to combat terrorism. Other agencies taking steps to improve their evaluations of exercises include the Department of Energy and the FBI.
To reduce duplication and leverage resources, we recommend that the Assistant to the President for Science and Technology complete efforts to develop a strategic plan for research and development to combat terrorism, coordinating this with federal agencies and state and local authorities.	Partially implemented. The National Strategy for Homeland Security includes a chapter on science and technology, which includes an initiative to coordinate research and development of the homeland security apparatus. The proposed Department of Homeland Security, working with the White House and other federal departments, would set the overall direction for homeland security research and development. The proposed department would also establish a network of national laboratories for homeland security. Given that the department is only a proposal at this time, it is too early to determine how it might implement our recommendation.
To eliminate overlapping assistance programs and to provide a single liaison for state and local officials, we recommend that the President, working closely with Congress, consolidate the activities of the FBI's National Domestic Preparedness Office and the Department of Justice's Office for State and Local Domestic Preparedness Support under FEMA.	Partially implemented. In June 2002, the President proposed that a new Department of Homeland Security take the lead for federal programs to assist state and local governments. Given that the department is only a proposal at this time, it is too early to determine whether these offices and their functions have been successfully consolidated.
To clarify the roles and missions of specialized National Guard response teams in a terrorist incident involving WMD, we recommend that the Secretary of Defense suspend the establishment of any additional National Guard Weapons of Mass Destruction Civil Support Teams until DOD has completed its coordination of the teams' roles and missions with the FBI. We also recommend that the Secretary of Defense reach a written agreement with the Director of the FBI that clarifies the roles of the teams in relation to the FBI.	Partially implemented. Subsequent to our earlier report on these teams, and a report by the DOD Inspector General, which found some similar problems, DOD agreed to review the National Guard teams and work with other agencies to clarify their roles in responding to terrorist incidents. In September 2001, DOD restricted the number of teams to 32.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
To strengthen the federal government's critical infrastructure strategy, we recommend that the Assistant to the President for National Security Affairs define • specific roles and responsibilities of organizations involved in critical infrastructure protection and related information security activities; • interim objectives and milestones for achieving CIP goals and a specific action plan for achieving these objectives, including implementation of vulnerability assessments and related remedial plans; and • performance measures for which entities can be held accountable.	Not implemented: The President's Critical Infrastructure Protection Board released a draft strategy on September 18, 2002, for comment. The draft does not specify roles and responsibilities, .or performance measures. However, the President's Critical Infrastructure Protection Board plans to periodically update the strategy as it evolves. The draft also states that other groups have developed strategies related to their portion of cyberspace they own or operate. Further, the President's national strategy for homeland security, issued in July 2002, states that a comprehensive national infrastructures plan will be issued in the future.
We believe the federal government's cyber-security strategy should be linked to the national strategy to combat terrorism. However, the two areas are different in that the threats to computer-based infrastructures are broader than terrorism and programs to protect them are more closely associated with traditional information security activities.	Regarding the link with efforts to combat terrorism, the draft strategy states that it supports both the National Strategy for Homeland Security and the National Security Strategy of the United States.

Homeland Security: Key Elements to Unify Efforts Are Underway but Uncertainty Remains (GAO-02-610, June 7, 2002).
Recommendations, p. 20.

GAO recommendations	Status of recommendations
We recommend that the President direct OHS to (1) develop a comprehensive, governmentwide definition of homeland security, and (2) include the definition in the forthcoming national strategy.	Implemented. In July 2002, OHS published the National Strategy for Homeland Security. In this document, there is a detailed definition of homeland security.

Nonproliferation R&D: NNSA's Program Develops Successful Technologies, but Project Management Can Be Strengthened (GAO-02-904, Aug. 23, 2002). Recommendations, pp. 20-21.

GAO recommendations	Status of recommendations
We recommend that the Administrator of the National Nuclear Security Administration (NNSA) work with OHS (or the Department of Homeland Security, if established) to clarify the Nonproliferation and Verification Research and Development Program's role in relation to other agencies conducting counterterrorism research and development and to achieve an appropriate balance between short-term and long-term research. In addition, to improve the program's ability to successfully transfer new technologies to users, the program should, in cooperation with OHS, allow users opportunities to provide input through all phases of research and development projects	Partially implemented. NNSA agreed to the recommendation and stated that it will improve coordination with other agencies conducting research and development. In addition, coordination may be improved if two of the program's divisions are moved to a new Department of Homeland Security, as proposed by the President.

Related GAO Products

Homeland Security

September 11: Interim Report on the Response of Charities. GAO-02-1037. Washington, D.C.: September 3, 2002.

National Preparedness: Technology and Information Sharing Challenges. GAO-02-1048R. Washington, D.C.: August 30, 2002.

Homeland Security: Effective Intergovernmental Coordination is Key to Success. GAO-02-1013T. Washington, D.C.: August 23, 2002.

Homeland Security: Effective Intergovernmental Coordination is Key to Success. GAO-02-1012T. Washington, D.C.: August 22, 2002.

Homeland Security: Effective Intergovernmental Coordination Is Key to Success. GAO-02-1011T. Washington, D.C.: August 20, 2002.

Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful. GAO-02-993T. Washington, D.C.: August 5, 2002.

Chemical Safety: Emergency Response Community Views on the Adequacy of Federally Required Chemical Information. GAO-02-799. Washington, D.C.: July 31, 2002.

Aviation Security: Transportation Security Administration Faces Immediate and Long-Term Challenges. GAO-02-971T. Washington, D.C.: July 25, 2002.

Critical Infrastructure Protection: Significant Challenges Need to Be Addressed, GAO-02-961T. Washington, D.C.: July 24, 2002.

Homeland Security: Critical Design and Implementation Issues. GAO-02-957T. Washington, D.C.: July 17, 2002.

Homeland Security: New Department Could Improve Coordination but Transferring Control of Certain Public Health Programs Raises Concerns. GAO-02-954T. Washington, D.C.: July 16, 2002.

Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach to Protecting Information Systems. GAO-02-474. Washington, D.C.: July 15, 2002.

Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed. GAO-02-918T. Washington, D.C.: July 9, 2002.

Homeland Security: New Department Could Improve Biomedical R&D Coordination but May Disrupt Dual-Purpose Efforts. GAO-02-924T. Washington, D.C.: July 9, 2002.

Homeland Security: Title III of the Homeland Security Act of 2002. GAO-02-927T. Washington, D.C.: July 9, 2002.

Homeland Security: Intergovernmental Coordination and Partnership Will Be Critical to Success. GAO-02-901T. Washington, D.C.: July 3, 2002.

Homeland Security: New Department Could Improve Coordination but May Complicate Priority Setting. GAO-02-893T. Washington, D.C.: June 28, 2002.

Homeland Security: New Department Could Improve Coordination but May Complicate Public Health Priority Setting. GAO-02-883T. Washington, D.C.: June 25, 2002.

Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will Be Pivotal to Success. GAO-02-886T. Washington, D.C.: June 25, 2002.

FBI Reorganization: Initial Steps Encouraging but Broad Transformation Needed. GAO-02-865T. Washington, D.C.: June 21, 2002.

Homeland Security: Key Elements to Unify Efforts Are Underway but Uncertainty Remains. GAO-02-610. Washington, D.C.: June 7, 2002.

National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy. GAO-02-811T. Washington, D.C.: June 7, 2002.

Review of Studies of the Economic Impact of the September 11, 2001, Terrorist Attacks on the World Trade Center. GAO-02-700R. Washington, D.C.: May 29, 2002.

Homeland Security: Integration of Federal, State, Local, and Private Sector Efforts Is Critical to an Effective National Strategy for Homeland Security. GAO-02-621T. Washington, D.C.: April 11, 2002.

Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy. GAO-02-549T. Washington, D.C.: March 28, 2002.

Homeland Security: Progress Made, More Direction and Partnership Sought. GAO-02-490T. Washington, D.C.: March 12, 2002.

Homeland Security: Challenges and Strategies in Addressing Short- and Long-Term National Needs. GAO-02-160T. Washington, D.C.: November 7, 2001.

Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts. GAO-02-208T. Washington, D.C.: October 31, 2001.

Homeland Security: Need to Consider VA's Role in Strengthening Federal Preparedness. GAO-02-145T. Washington, D.C.: October 15, 2001.

Homeland Security: Key Elements of a Risk Management Approach. GAO-02-150T. Washington, D.C.: October 12, 2001.

Homeland Security: A Framework for Addressing the Nation's Issues. GAO-01-1158T. Washington, D.C.: September 21, 2001.

Combating Terrorism

Chemical Weapons: Lessons Learned Program Generally Effective but Could Be Improved and Expanded. GAO-02-890. Washington, D.C.: September 10, 2002.

Combating Terrorism: Department of State Programs to Combat Terrorism Abroad. GAO-02-1021. Washington, D.C.: September 6, 2002.

Export Controls: Department of Commerce Controls over Transfers of Technology to Foreign Nationals Need Improvement. GAO-02-972. Washington, D.C.: September 6, 2002.

Nonproliferation R&D: NNSA's Program Develops Successful Technologies, but Project Management Can Be Strengthened. GAO-02-904. Washington, D.C.: August 23, 2002.

Diffuse Security Threats: USPS Air Filtration Systems Need More Testing and Cost Benefit Analysis Before Implementation. GAO-02-838. Washington, D.C.: August 22, 2002.

Nuclear Nonproliferation: U.S. Efforts to Combat Nuclear Smuggling. GAO-02-989T. Washington, D.C.: July 30, 2002.

Combating Terrorism: Preliminary Observations on Weaknesses in Force Protection for DOD Deployments Through Domestic Seaports. GAO-02-955TNI. Washington, D.C.: July 23, 2002.

Diffuse Security Threats: Technologies for Mail Sanitization Exist, but Challenges Remain. GAO-02-365. Washington, D.C.: April 23, 2002.

Combating Terrorism: Intergovernmental Cooperation in the Development of a National Strategy to Enhance State and Local Preparedness. GAO-02-550T. Washington, D.C.: April 2, 2002.

Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy. GAO-02-549T. Washington, D.C.: March 28, 2002.

Combating Terrorism: Critical Components of a National Strategy to Enhance State and Local Preparedness. GAO-02-548T. Washington, D.C.: March 25, 2002.

Combating Terrorism: Intergovernmental Partnership in a National Strategy to Enhance State and Local Preparedness. GAO-02-547T. Washington, D.C.: March 22, 2002.

Combating Terrorism: Key Aspects of a National Strategy to Enhance State and Local Preparedness. GAO-02-473T. Washington, D.C.: March 1, 2002.

Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness. GAO-01-162T. Washington, D.C.: October 17, 2001.

Combating Terrorism: Selected Challenges and Related Recommendations. GAO-01-822. Washington, D.C.: September 20, 2001.

Combating Terrorism: Actions Needed to Improve DOD's Antiterrorism Program Implementation and Management. GAO-01-909. Washington, D.C.: September 19, 2001.

Combating Terrorism: Comments on H.R. 525 to Create a President's Council on Domestic Preparedness. GAO-01-555T. Washington, D.C.: May 9, 2001.

Combating Terrorism: Observations on Options to Improve the Federal Response. GAO-01-660T. Washington, D.C.: April 24, 2001.

Combating Terrorism: Comments on Counterterrorism Leadership and National Strategy. GAO-01-556T. Washington, D.C.: March 27, 2001.

Combating Terrorism: FEMA Continues to Make Progress in Coordinating Preparedness and Response. GAO-01-15. Washington, D.C.: March 20, 2001.

Combating Terrorism: Federal Response Teams Provide Varied Capabilities; Opportunities Remain to Improve Coordination. GAO-01-14. Washington, D.C.: November 30, 2000.

Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training. GAO/NSIAD-00-64. Washington, D.C.: March 21, 2000.

Combating Terrorism: Observations on the Threat of Chemical and Biological Terrorism. GAO/T-NSIAD-00-50. Washington, D.C.: October 20, 1999.

Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attack. GAO/NSIAD-99-163. Washington, D.C.: September 7, 1999.

Combating Terrorism: Observations on Growth in Federal Programs. GAO/T-NSIAD-99-181. Washington, D.C.: June 9, 1999.

Combating Terrorism: Analysis of Potential Emergency Response Equipment and Sustainment Costs. GAO-NSIAD-99-151. Washington, D.C.: June 9, 1999.

Combating Terrorism: Use of National Guard Response Teams Is Unclear. GAO/NSIAD-99-110. Washington, D.C.: May 21, 1999.

Combating Terrorism: Observations on Federal Spending to Combat Terrorism. GAO/T-NSIAD/GGD-99-107. Washington, D.C.: March 11, 1999.

Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency. GAO-NSIAD-99-3. Washington, D.C.: November 12, 1998.

Combating Terrorism: Observations on the Nunn-Lugar-Domenici Domestic Preparedness Program. GAO/T-NSIAD-99-16. Washington, D.C.: October 2, 1998.

Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments. GAO/NSIAD-98-74. Washington, D.C.: April 9, 1998.

Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination. GAO/NSIAD-98-39. Washington, D.C.: December 1, 1997.

Public Health

Public Health: Maintaining an Adequate Blood Supply Is Key to Emergency Preparedness. GAO-02-1095T. Washington, D.C.: September 10, 2002.

Homeland Security: New Department Could Improve Coordination But May Complicate Public Health Priority Setting. GAO-02-883T. Washington, D.C.: June 25, 2002.

Bioterrorism: The Centers for Disease Control and Prevention's Role in Public Health Protection. GAO-02-235T. Washington, D.C.: November 15, 2001.

Bioterrorism: Review of Public Health and Medical Preparedness. GAO-02-149T. Washington, D.C.: October 10, 2001.

Bioterrorism: Public Health and Medical Preparedness. GAO-02-141T. Washington, D.C.: October 10, 2001.

Bioterrorism: Coordination and Preparedness. GAO-02-129T. Washington, D.C.: October 5, 2001.

Bioterrorism: Federal Research and Preparedness Activities. GAO-01-915. Washington, D.C.: September 28, 2001.

Chemical and Biological Defense: Improved Risk Assessments and Inventory Management Are Needed. GAO-01-667. Washington, D.C.: September 28, 2001.

West Nile Virus Outbreak: Lessons for Public Health Preparedness. GAO/HEHS-00-180. Washington, D.C.: September 11, 2000.

Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks. GAO/NSIAD-99-163. Washington, D.C.: September 7, 1999.

Chemical and Biological Defense: Program Planning and Evaluation Should Follow Results Act Framework. GAO/NSIAD-99-159. Washington, D.C.: August 16, 1999.

Combating Terrorism: Observations on Biological Terrorism and Public Health Initiatives. GAO/T-NSIAD-99-112. Washington, D.C.: March 16, 1999.

Disaster Assistance

Disaster Assistance: Improvement Needed in Disaster Declaration Criteria and Eligibility Assurance Procedures. GAO-01-837. Washington, D.C.: August 31, 2001.

FEMA and Army Must Be Proactive in Preparing States for Emergencies. GAO-01-850. Washington, D.C.: August 13, 2001.

Federal Emergency Management Agency: Status of Achieving Key Outcomes and Addressing Major Management Challenges. GAO-01-832. Washington, D.C.: July 9, 2001.

Budget and Management

Performance Budgeting: Opportunities and Challenges. GAO-02-1106T. Washington, D.C.: September 19, 2002.

Electronic Government: Proposal Addresses Critical Challenges. GAO-02-1083T. Washington, D.C.: September 18, 2002.

Results-Oriented Cultures: Insights for U.S. Agencies from Other Countries' Performance Management Initiatives. GAO-02-862. Washington, D.C.: August 2, 2002.

Acquisition Workforce: Agencies Need to Better Define and Track the Training of Their Employees. GAO-02-737. Washington, D.C.: July 29, 2002.

Managing for Results: Using Strategic Human Capital Management to Drive Transformational Change. GAO-02-940T. Washington, D.C.: July 15, 2002.

Coast Guard: Budget and Management Challenges for 2003 and Beyond. GAO-02-538T. Washington, D.C.: March 19, 2002.

A Model of Strategic Human Capital Management. GAO-02-373SP. Washington, D.C.: March 15, 2002.

Budget Issues: Long-Term Fiscal Challenges. GAO-02-467T. Washington, D.C.: February 27, 2002.

Managing for Results: Progress in Linking Performance Plans with Budget and Financial Statements. GAO-02-236. Washington, D.C.: January 4, 2002.

Results-Oriented Budget Practices in Federal Agencies. GAO-01-1084SP. Washington, D.C.: August 2001.

Managing for Results: Federal Managers' Views on Key Management Issues Vary Widely across Agencies. GAO-01-0592. Washington, D.C.: May 2001.

Determining Performance and Accountability Challenges and High Risks. GAO-01-159SP. Washington, D.C.: November 2000.

Managing for Results: Using the Results Act to Address Mission Fragmentation and Program Overlap. GAO/AIMD-97-156. Washington, D.C.: August 29, 1997.

Government Restructuring: Identifying Potential Duplication in Federal Missions and Approaches. GAO/T-AIMD-95-161. Washington, D.C.: June 7, 1995.

Grant Design

Grant Programs: Design Features Shape Flexibility, Accountability, and Performance Information. GAO/GGD-98-137. Washington, D.C.: June 22, 1998.

Federal Grants: Design Improvements Could Help Federal Resources Go Further. GAO/AIMD-97-7. Washington, D.C.: December 18, 1996.

Block Grants: Issues in Designing Accountability Provisions. GAO/AIMD-95-226. Washington, D.C.: September 1, 1995.

STATEMENT FOR THE RECORD

FOR

THE JOINT 9/11 INQUIRY

1 October 2002

INFORMATION SHARING OF TERRORISM-RELATED DATA

Rear Admiral Lowell E. Jacoby, USN
Acting Director, Defense Intelligence Agency

Statement for the Record
Rear Admiral Lowell E. Jacoby, United States Navy
Acting Director, Defense Intelligence Agency
1 October 2002

Chairman Graham, Chairman Goss, and Members of these Committees, thank you for the opportunity to address the issue of sharing terrorism-related information. It is a topic of exceptional importance and one upon which DIA has focused considerable attention in an effort to enhance our analytic approach and capabilities for the war on terrorism. As requested, this statement is structured around the specific questions contained in your September 17, 2002, letter.

Very shortly after the terrorist attack on the USS COLE in October 2000, DIA took steps to significantly alter its structures, processes, products, and conventions associated with analysis of terrorism. We recognized at that time that the terrorist threat had evolved and changed in very complex ways and that our analytic approach had not kept pace with those changes. The steps we took were based on two fundamental beliefs: that analysis, conducted in true all-source mode, could make greater contributions to the counterterrorism mission; and that significant amounts of information with relevance to the terrorist threat were under-utilized, essentially not subjected to analytic scrutiny and exploitation.

We understood that we were not optimally configured – in terms of policies, procedures, and technology – to accommodate the receipt and rapid exploitation of that under-tapped information. Consequently, we fielded the mechanisms needed to obviate several factors that had limited our ability to receive some categories of information. These factors ranged from strict compartmentation and law enforcement concerns to sheer volume and fragmentation of data . With the standup of the Joint Intelligence Task Force for Combating Terrorism (JITF-CT) and its associated "limited access data repositories," leading-edge information handling technology, and consolidated analytic cadre, we are close to being optimally configured to receive information from any and all sources.

The JITF-CT is a consolidated national-level Department of Defense (DOD) all-source intelligence fusion center staffed, equipped, and directed to support an aggressive, long-term, worldwide campaign against terrorism. The JITF-CT is designed to support the full range of DOD efforts to combat terrorism, both offensive and defensive, with particular focus on providing strategic and tactical warning, exposing and exploiting terrorist vulnerabilities, and preventing terrorists and their sponsors from acquiring increased capabilities, particularly in the area of weapons of mass destruction.

The single most critical goal of the JITF-CT is fielding of a stand-alone, limited access data repository accredited to host the entire range of terrorism-related

information, regardless of source. No such repository of information exists within the Department of Defense today. Categories of information often not subjected to all-source intelligence analysis today include some highly compartmented intelligence, law enforcement information related to ongoing investigations or prosecutions, and security incident reporting sometimes catalogued as criminal, rather than terrorism activity.

The JITF-CT intends to not only capture this information but to apply state-of-the-practice technological tools and expertise that enhance opportunities for "analytic discovery." For example, commercially-available tools can help discern and understand obscure linkages between individuals, activities, and methods in the pre-attack phase of a terrorist operation, even if it stretches over years and several continents. Using commercial technology, the JITF-CT will sustain a terrorism analysis effort that dramatically modernizes the way it accesses, stores, manipulates, interprets, and disseminates information.

Successes in deterring terrorist attacks will most always involve some combination of intelligence, good police of investigative work, vigilant security, foreign government involvement, and plain luck. With the exception of luck, each of these entities possesses knowledge and information not ordinarily available to the intelligence analyst. Trends in terrorist organizational and operational behavior – loosely affiliated groups and collaborative planning or execution of operations, often geographically dispersed and stretching over long periods of time – combined with their small footprint and extraordinary efforts to conceal their activities argue that terrorism-related information will nearly always appear to be fragmentary, ambiguous, and uncorroborated.

In our search for relevant information, we must cast a much wider net and then more rigorously mine, manipulate, and interpret the take. In terms of the now-popular analogy of "connecting the dots," we must assume that some of those "dots" are to be found in the observations of gate guards, investigations of thefts and break-ins, or the seemingly benign conversations between terrorist supporters and sympathizers. We simply cannot allow a "dot" to be overlooked, regardless of where it might be found or how deeply embedded in noise or obscured by faulty assumptions about its nature and relevance.

At its most basic, intelligence analysis is a relatively binary process wherein evidence – observed, reported facts/activities – is combined with assumptions – analytic insight, knowledge – to create an assessment. In essence, the terrorism analyst's job is the extraction of "meaning" from incomplete evidence, using knowledge, experience, expertise and insight to compensate for absent evidence and ever-present ambiguity.

As more powerful and diverse assumptions are applied to the evidentiary base, more powerful and precise assessments are produced. The only certain way to increase the breadth and diversity of assumptions is to increase the breadth and diversity (in terms of educational and experiential background, cultural values,

intellectual biases, etc.) of the analysts involved in the assessment process. In this regard, the more widely fragmentary information is shared, the more likely its hidden meaning will be revealed. Information considered irrelevant noise by one set of analysts may provide critical clues or reveal significant relationships when subjected to analytic scrutiny by another. This process is critical for the terrorism issue where evidence is particularly scant, often separated by space and time.

As an active and vocal advocate of collaborative analysis and increased sharing of information, DIA knows the importance of close community cooperation and is an active participant in the terrorism intelligence community. We have backed up our commitment to analytic partnership by assigning experienced terrorism analysts to other counterterrorism organizations. We currently have analysts deployed in support of interrogation efforts in Afghanistan and at Guantanamo Bay. The JITF-CT has experienced terrorism analysts assigned to counterterrorism components of the CIA, FBI and NSA. As new personnel are hired and trained, we will begin deploying JITF-CT terrorism analysts to the Combatant Command Joint Intelligence Centers.

Of note, the JITF-CT charter lists "Bridging Interagency Terrorism Intelligence Efforts" as one of its primary functions. Through assignment of JITF-CT personnel to, and hosting personnel from, other U.S. government elements engaged in the campaign against terrorism, the JITF-CT seeks to ensure DOD is aware of and able to assist, benefit from, and coordinate relevant antiterrorism and counterterrorism intelligence efforts throughout the U.S. government. In this regard, DIA maintains longstanding and active participation in the Interagency Intelligence Committee on Terrorism.

Historically, we've had mixed results regarding the effectiveness of community partnerships. The mere act of assigning an analyst to another organization does not ensure a greater level of access to information or more open sharing of information. JITF-CT analysts in counterpart organizations do not have unfettered and unconditional access to all relevant terrorist information. By virtue of their status, these analysts are unquestionably afforded greater access to host agency data, but, in some cases, they are restricted from making that additional information available to colleagues at their home agency. As such, some of the tangible benefits and explicit objectives of exchanging personnel – sharing of information and leveraging collective expertise – are degraded. However, real progress has been made in the past year and I am optimistic that the full benefits and objectives of community integration will ultimately be realized.

In response to your specific question about information sharing, DIA does not have access to all intelligence and law enforcement information on terrorists. I cannot quantitatively or qualitatively assess the percentage of "missing" information; I can't know what I don't know. Nor can I precisely describe the limits or the basis for those limitations regarding information that is withheld from DIA. I respectfully suggest that explanations should more appropriately come from those intelligence and law enforcement organizations that are the "owners" or "arbiters" of unshared information. That being said, I want to emphasize that I do not believe any information "owner" has failed to rapidly share even a shred of information that it deems as conveying either an

explicit or implicit threat to United States citizens or activities. I believe the unshared information falls largely into the categories of background of contextual data, sourcing, seemingly benign activities, and the like. But, as previously mentioned, it is within these categories that the critical "connecting dot" may well be found.

Also in response to one of your specific questions, I am not aware of any legal or policy obstacle to DIA sharing information related to terrorism, suspected terrorists, and their associates. We are, of course, subject to a range of intelligence oversight policies and procedures that impose some restrictions, most notably those pertaining to United States citizens, but we are not constrained from performing our foreign intelligence or force protections missions. Laws and governing directives provide sufficient flexibility and, properly interpreted and complied with, do not inhibit our ability to share or receive information relevant to the terrorist threat.

DIA has a longstanding commitment to share and widely disseminate the results of its terrorism analysis. The JITF-CT currently maintains an extensive terrorism data base that dates back to the mid-1980s and fulfills intelligence production responsibilities established in DOD directives. This data base was established principally to provide our customers with baseline terrorist threat and modus operandi analysis in support of the force protection (antiterrorism, prevention) mission. It is neither designed nor used for tracking suspected terrorist movements in the United States or abroad. The finished intelligence contained in our data base – for example, over 10,000 biographic profiles, 190 terrorist group profiles, over 8,000 incident summaries, and current threat assessments for every country in the world – is available on-line to anyone with access to DOD intelligence networks. As you can imagine, this represents a serious resource investment that underscores our deep commitment to information sharing.

During my interview with the Joint Inquiry Staff, I stated that one significant change needed was to create a new paradigm wherein "ownership" of information belonged with the analysts and not the collectors. In my opinion, one of the most prolonged and troubling trends in the intelligence community is the degree to which analysts – while being expected to incorporate the full range of source information into their assessments – have been systematically separated from the raw material of their trade. In fact, while I acknowledge there are many pockets where groundbreaking, innovative, true all-source analysis is occurring, they are the exception, not the rule. I don't make this statement lightly and it is not my intent to offend or disparage the quality of our analysts or the competence of their management, because – of course – I'm part of that latter group.

There are good and very understandable reasons why our all-source analysis effort is in this situation. Large analytic workforce drawdowns of the early 90s, combined with voluminous streams of collected data required more "front end" filtering of raw information, thus moving the interpretive functions of analysis – the extraction of meaning from data – further inside the collecting organizations. This is not necessarily a bad thing. And, I have great respect for those in the processing and exploitation

arena who labor to separate the nuggets from the noise, to rationalize the irrational, and to add meaning. Theirs is an indispensable and value-adding function.

However, when so-called all-source analysts are put in the position of basing important judgments on "some-source" or "already-interpreted-source" information, that is a bad thing. I need to be clear in stating that I am referring to access to collected data, not unfettered access to source data, particularly the areas of law enforcement and human sources. On exceptionally difficult issues such as terrorism analysis, where the available information is by its very nature fragmentary and episodic, we need to find a way to immediately and emphatically put the "all" back into all-source analysis.

If we expect analysts to perform at the level and speed expected in a counterterrorism mission environment characterized by pop-up threats, fleeting targets, and heavily veiled communication, they require immediate, on-demand access to data from all sources and the ability to mine, manipulate, integrate, and display all relevant information. What I envision is a different way of doing business in the intelligence and law enforcement communities. Make no mistake; it would involve unfamiliar processes, partnership, and prerogatives.

While broad access to data is one of the keys to changing the paradigm, another important step is more effective management and exploitation of information. Before we can field successful information management strategies, we must first put our information in a form and into an environment where it can, in fact, be managed.

Information Management is an area where we should take our lead from the commercial sector. After all, profits and losses of information-fueled business outside of government are determined by how they manage information. Those who are successful in a business sense – showing real rather than paper profit – certainly have some lessons to teach us.

If we are to achieve an end state characterized by the ability to rapidly share and integrate information, we must move toward a common data framework and set of standards that will allow interoperability – at the data, not system, level. In my view, the commercial world's collective embrace of eXtensible Markup Language – XML – standards is precisely what we should do. And, the sooner the better, not just for a limited group of intelligence producers and subsets of data; it shouldn't be an elective option. Interoperability at the data level is an absolutely necessary attribute of a transformed intelligence environment because it enables horizontal integration of information from all sources – not just intelligence – and at all levels of classification.

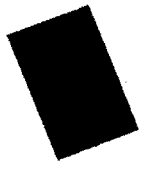
Since 11 September 2001, there have been significant improvements in a number of areas related to information sharing. DIA has made notable arrangements with other intelligence community partners to achieve new levels of data access and integration. In other cases, we still have work to do both technologically and procedurally within the JITF-CT and in breaking down external barriers to full sharing.

But, I am exceptionally optimistic. The Director of Central Intelligence expressed his commitment by emphasizing that full sharing of unfiltered, aggregated, and interpreted collected information is a necessary ingredient for victory in the war on terrorism and that anything short of full sharing of such information ultimately hampers our ability to protect the citizens and interests of the United States. I'm with him.

FOR OFFICIAL USE ONLY

UNTIL RELEASED BY THE SENATE SELECT COMMITTEE ON INTELLIGENCE AND

THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE



STATEMENT OF

DR. ROBERT C. NORRIS, JR.

CHAIR, INFORMATION OPERATIONS AND TECHNOLOGY DEPARTMENT

NATIONAL DEFENSE UNIVERSITY

BEFORE THE

SENATE SELECT COMMITTEE ON INTELLIGENCE AND

THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE JOINT INQUIRY

ON

SYSTEMIC ISSUES OF INFORMATION SHARING OF TERRORISM-RELATED DATA

1 OCTOBER 2002

FOR OFFICIAL USE ONLY

UNTIL RELEASED BY THE SENATE SELECT COMMITTEE ON INTELLIGENCE AND

THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

Introduction

Chairman Graham, Senator Shelby, Chairman Goss, Congresswoman Pelosi, and members of the Joint Inquiry, I have been asked to reply to four questions about information technology architecture, or enterprise architecture (EA), that touch on the issues of data and information sharing for counterterrorism. By extension, this topic includes interoperability, knowledge management (KM), and collaboration.

Interoperability is the ability of information systems to access, manipulate, and exchange information between multiple disparate systems. A system that can exchange information and services with multiple systems is described as more interoperable than one that cannot. The ability of systems to accomplish these interactions with other fielded information systems is paramount to DoD users (1). Interoperability implies that a product supports user understanding of the data and, therefore, the ability to utilize the data.

Knowledge Management, according to Gartner, is a business process for the management of an enterprise's intellectual assets. It is a discipline that promotes an integrated and collaborative approach to the creation, capture, organization, access and use of information assets (2). *Webster* defines collaboration as working jointly with others especially in an intellectual endeavor

I have woven these concepts into my response to your questions since they are related to systemic issues about information sharing of terrorism-related data.

1. What are the key elements of information technology architecture to facilitate information sharing of terrorism-related data, especially if the information is in multiple data bases in

different agencies, needs to be protected and secured from unauthorized access, or is classified?

An EA is a comprehensive model of an enterprise: a master plan, which acts as a planning, structuring, and integrating guideline and force for an organization. EA covers business structure and context, information technology dimension and organizational structure, and workflow dimension in achieving the organization's goals and strategies. Rapidly changing environments demand more flexible and adaptable information systems infrastructure. However, synchronizing enterprise goals and strategies; IT governance; organizational structures, processes, and data; business applications, their systems and data bases; and network infrastructure become more critical (3). It is difficult to synchronize processes, data, applications, and data bases when you have several competing EA frameworks.

The DoD is in the latest iteration of its EA framework, which is an expansion, clarification, and maturing of the concepts presented in the C4ISR[1] Architecture Framework, Version 2.0. I understand that the National Reconnaissance Office has developed a version of the DoD EA framework tailored for their use.

The Intelligence Community[2] (IC) is made up, in part, by components of DoD. Its IC System for Information Sharing (ICSIS) is their future architecture. This architecture is planned to allow (but does not require) IC member organizations to establish an organizational shared space where they can share data and applications

[1] C4ISR = Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.
[2] The Intelligence Community is composed of 13 agencies across the Federal Government and headed by the Director of Central Intelligence.

within the IC while maintaining the direct protection and control over those resources. ICSIS will be implemented in a phased approach over the next 10 years. However, it is important to note that the January 2001 NIMA[3] Commission report recommended that that agency, part of the IC and DoD, develop a new EA from a clean sheet (4).

The Federal Government also has developed an EA framework. It is worthwhile to review the development status of this EA since it is well recognized that the DoD and the other Federal agencies will need to share data and information, and integrate applications, for effective counterterrorism activities.

In September 1999, the Chief Information Officers Council issued the Federal Enterprise Architecture Framework, Version 1.1.

> "The Framework consists of various approaches, models, and definitions for communicating the overall organization and relationships of architecture components required for developing and maintaining a Federal Enterprise Architecture...The architecture will serve as a reference point to facilitate the efficient and effective coordination of common business processes, information flows, systems, and investments among Federal Agencies and other Governmental entities."

The framework identified three approaches to developing the EA but I will mention only the two actually considered. The "conventional approach" requires a substantial initial investment in time and dollars and results in a common baseline, or current architecture, for all federal enterprises. The Federal Government would have to specify the detailed description of a target or "to be" architecture for all

[3] NIMA = National Imagery and Mapping Agency

agencies and the development of a transition plan to achieve it—before design, development, and acquisition of new systems could occur.

An alternative "segment approach" was proposed by the Federal CIOs for developing the EA. The architecture is incrementally developed by focusing on common functions or specific enterprises. This approach was considered by them to be more cost-effective and flexible. In May 1999, the CIO Council drafted a process for identifying and approving Federal segments. These segments will be developed individually and integrated into a larger EA at some future point.

This framework envisions the Federal EA having a data architecture, an applications architecture, and a technology architecture based on five reference models. These models would facilitate "cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across Federal agencies (5)." The Federal EA Program Management Office has identified the following models, listed at http://www.feapmo.gov:

- The Business Reference Model (BRM) provides an organized, hierarchical construct for describing day-to-day operations in the Federal Government. This model was released in July 2002. It comprises 37 pages and is a high-level view of services to citizens, support delivery of services, and internal operations and infrastructure.
- The Performance Reference Model (PRM) is a framework for performance measurement that provides common application measures throughout the Federal Government. It allows agencies to better manage the business of government at a federal strategic level while providing a means

for gauging progress towards the target FEA. It is expected later this year with no fixed date.

- The Application-Capability Reference Model (ARM) will identify and classify horizontal and vertical IT application capabilities that support Federal agencies. The model will aid in recommending applications to support the reuse of business components and services across the Federal Government. It is expected later this year with no fixed date.
- The Technical Reference Model (TRM) is a hierarchical foundation to describe how technology is supporting the delivery of the application capability. The TRM will outline the technology elements that collectively support the adoption and implementation of component-based architectures. It is expected later this year with no fixed date.
- The Data and Information Reference Model (DRM) will describe, at an aggregate level, the data and information that support program and business line operations. The model will aid in describing the types of interaction and exchanges that occur between the Federal Government and its various customers, constituencies, and business partners. There is no release date for this model.

These models are necessary precursors to the development of the data, applications, and technology architectures for the Federal EA. Since only <u>one</u> of the five models exists today, it can be assumed that a Federal EA will not be complete until sometime in the future. While all the models are important, I believe the DRM is the <u>key</u> to efficient and effective data and information sharing.

Brigadier General Michael Ennis, director of intelligence at US Marine Corps headquarters, was quoted in *Federal Computer Week* as saying, "Interoperability begins at the data level, not the systems level (9/16/02)." Defining the data for an EA is hard work today and is usually done last--if at all. Many organizations encounter turf battles about who owns the data and who gets to define and describe it. However, the need to define and describe data is not new.

Whenever you write a computer program, you have to define the data by type and length. Unfortunately, early computer programming required writing this data description within the program source code (the instructions that make the program perform). The data description was then stove-piped within the computer program and a multitude of data descriptions for the same term appeared within an enterprise. Instead of one data description for "First Name" being text data of 20 characters in length, we have many of varying lengths. Therein lies the problem: whose data description and definition will prevail. And when it comes to intelligence work, it is very important to have an agreed upon definition so everyone understands the data.

The data model is important to EA. Gartner notes that the "centerpiece" for integrating applications and sharing data, is to model the data to be exchanged between independently developed application systems (6). To the best of their knowledge, no government or enterprise has a detailed, enterprise-wide application integration repository for holding a comprehensive exchange information model. Gartner also notes the relationship between knowledge management and the EA Data Model by saying (2):

> "KM cannot be supported simply by amalgamation of a mass of data; it requires the structuring and navigation supported by metadata—the formal description of data and its inter-

relationships. KM relies on metadata about physical structures or data types, access methods, and about content."

The second part of Question 1 asks: What are the key elements of an EA if the data needs to be protected and secured from unauthorized access, or is classified? Again, the key element is accurate data and information definitions so that national security data and information can be correctly identified and tagged as to its classification level.

2. How is the Department of Defense (DoD) implementing information assurance architecture to protect digital information but yet, also make it available to those that need the information? Has the DoD been effective in achieving both goals and what are the implications for a DoD-wide or government-wide enterprise architecture for counterterrorism?

It is a well-known fact that information assurance architectures should be designed into computer hardware or software products up-front and not as an afterthought. Our current experience with continually installing security patches on operating systems and computer applications shows that today's Commercial Off-the-Shelf (COTS) products are playing catch-up on information assurance architectures.

The DoD uses a combination of COTS products and government developed computer applications. The DoD, in accordance with National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, requires that COTS products used to enter, process, store, display, or transmit national security information be evaluated in accordance with the Common Criteria. This is an international standard for evaluating information assurance (7). The DoD has

promulgated instructions to all personnel to implement this requirement, DoD Instruction 8500.bb.

In my opinion, a properly developed Common Criteria Protection Profile, the description of how the technology will provide information assurance, should permit computer products to be evaluated for protecting digital information and also make the information available to those who need it for counterterrorism. Since NSTISSP No. 11 became a DoD requirement on 1 July 2002, it is too soon to determine if it is achieving information protection and/or inhibiting data sharing.

DoD also has the Defense Information Technology Security Certification and Accreditation Program (DITSCAP-DoD Instruction 5200.40) for developing unclassified and classified information technology applications. This system development methodology evaluates whether a system is meeting the requirements of its System Security Authorization Agreement during the definition, verification, validation, and post-accreditation phases of system development. When the system is properly developed and accredited, a Designated Approving Authority (DAA) signs off on the authorization to operate or issues an Interim Authority to Operate until the system is corrected. The DAA is a senior military leader who has the authority to fund needed security improvements or stop the operation of the system (9).

We know that there are people, process, and technology issues associated with protecting digital information and making it available to those that have a need for it. I am unable to personally gauge how effective the DoD has been in achieving the objectives of information assurance and information sharing because I have not researched this specific topic through surveys or other means. However, if these objectives cannot be met, the implications are either not protecting

vital information or denying it to analysts and decision-makers who need it for homeland security.

3. What are the key policy and technical impediments to implementing effective information architecture that facilitates information sharing between agencies? Can these impediments affect the possible development of effective counterterrorism related information technology architecture in the DoD?

Lieutenant General Peter Cuviello, the US Army's Chief Information Officer, was quoted in *Federal Computer Week* (9/16/02) as saying: "'We're so fixated with systems, programs and products and then we talk about data, information and knowledge, but we attack it through system interoperability. We'll never get there with all interoperable systems,' because that would require everyone to use the same products, which will never happen." To me, the "products" are the Information Technology systems and they can be different, but we are generally using the same data for them with no common definitions.

I have identified that there are several architecture frameworks in existence in the Federal Government, DoD, and the IC. To paraphrase Lieutenant General Cuviello, "We're so fixated with architecture frameworks and then we talk about data…" In my opinion, it will be difficult to have interoperable systems as long as everyone has their own architecture and no common data model. One DoD-related group that understood this relationship was the Independent NIMA Commission when they stated in their report, "In developing an architecture for the NIMA database a rigorous data model inherently comes first. All other decisions (such as the systems model) ought to follow, not lead (4)."

The time has come to have a policy about which architecture framework is the framework. Then it is important to complete the Enterprise Architecture and properly maintain it. The EA data model has to be constructed to the needed degree of granularity—not to some unknown "aggregate."

The lack of a controlling EA makes sharing data for counterterrorism makes collaboration among analysts and decision makers difficult. As I understand it, the IC does not expect to realize a full collaborative information technological capability until 2005. Until that occurs, we could expect the following impediments to effective counterterrorism:

- Insufficient agility in the workplace;
- Inability to deliver tailored products and services in a timely manner;
- Large infrastructure costs;
- Lack of cooperation;
- Inability to share data and analysis results across several intelligence disciplines;
- Inability to respond as effectively as we could to crises; and
- Inferior ability to mine data.

These deficiencies flow, in part, from not having an EA. For example, I have heard that the Defense Information Systems Agency suggests that system developers should have common representations for 20 percent of the data to satisfy 80 percent of the requirements. To me, this means that we cannot even come to agreement on half the data definitions; thus, the data model will always be largely incomplete.

This is not a technical impediment but the need for strong direction from the top to get the job done.

4. What Federal agencies or private companies are at the forefront of information technology and can serve as models for information sharing of sensitive data to assist in the war against terrorism?

The General Accounting Office issued a report earlier this year on Enterprise Architecture (GAO-02-6) that examined the maturity of 116 Federal agencies in developing an EA. This report identified five stages of EA maturity:

Stage 1: Creating EA Awareness

Stage 2: Building the EA Management Foundation

Stage 3: Developing Architecture Products

Stage 4: Completing Architecture Products

Stage 5: Leveraging the EA for Managing Change

Only one Federal agency was identified as being at Stage 5—the U.S. Customs Service. DoD and IC agencies were determined by GAO to be at the following EA maturity stages:

Agency	EA Maturity Stage
Department of Defense	3
Department of the Army	4
Department of the Air Force	3
Department of the Navy	2
Defense Intelligence Agency	2
National Imagery and Mapping Agency	2
National Security Agency	2
U.S. Marine Corps	1

Agency	EA Maturity Stage
Defense Advanced Research Projects Agency	1
Department of State	3
Department of Energy	2
Central Intelligence Agency	1
Department of the Treasury	1
Federal Bureau of Investigation	1

Source: GAO-02-6

The US Customs Service and the Department of the Army could serve as models from within the Federal Government.

Regarding private companies that could serve as models, rather than mention specific companies, I would recommend looking at the financial services industry. This industry has had to adapt its information technology to regulatory and market pressure. It would be beneficial to identify the hardware and software manufacturers, and IT services companies that have worked with the financial services leaders to enable them to share sensitive data and be flexible in today's environment. Gartner has reported that approximately 60% of retail banks with deposits of more than $1 billion have a documented Enterprise Architecture (9).

Conclusion

This concludes my statement on Enterprise Architecture issues related to counterterrorism. Thank you for this opportunity to contribute to the war on terrorism.

References

1. Information Integration & Interoperability Directorate, ASDC3I, DoD, *Levels of Information Systems Interoperability: A Maturity Model Process for Assessing Architecture Requirements and Solutions*, 10 July 2002, retrieved from http://web2.deskbook.osd.mil on 24 September 2002.
2. Gartner Strategic Analysis Report, *The Impact of Knowledge Management on Enterprise Architecture*, R-09-6188, 25 October 1999.
3. Chung, H. M. and McLeod, G. Enterprise Architecture, Implementation, and Infrastructure Management, *Proceedings of the 35th Hawaii International Conference on System Sciences*, 2002.
4. *Report of the Independent Commission on the National Imagery and Mapping Agency*, January 2001, retrieved from http://www.fas.org/irp/agency/nima/ commission/ on 22 September 2002.
5. Chief Information Officers Council, *Federal Enterprise Architecture Framework*, Version 1.1, September 1999.
6. Gartner Research Note, *Government Insights: Tackling Data Integration Challenges*, COM-16-2732, 13 May 2002.
7. Common Criteria, Version 2.1, retrieved from http://csrc.nist.gov/cc/.
8. DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 1997, retrieved from http://iase.disa.mil/ditscap/ on 22 September 2002.
9. Gartner Research Note, *Adopting a Flexible Approach to Enterprise Architecture*, COM-17-7431, 26 August 2002

Chairman GRAHAM. Without objection, so ordered. Members of the committee may submit questions for the record to follow up on matters appropriately addressed to them. Further opening statements, Chairman Goss?

Chairman GOSS. Thank you very much, Mr. Chairman. We have had very successful hearings so far in the public that judging from the response we're seeing in the media and TV, printed media, that this is a value of what we are doing and we are very appreciative of our witnesses who are coming forward to help us with our chore of understanding better the consumer side of this and what the needs are at the levels of so many of our agencies who we entrust to do so much important work for the Nation in regard to national security.

I look forward to the hearing and I have no further statement except to express gratitude for those who are here with us today.

Chairman GRAHAM. Thank you, Congressman Goss. We will commence today with another in a series of excellent presentations by the Joint Inquiry Committee staff. Our staff director, Ms. Eleanor Hill is now recognized for her report.

[The prepared statement of Ms. Hill follows:]

Counterterrorism Information Sharing With Other Federal Agencies and with State and Local Governments and the Private Sector

Eleanor Hill, Staff Director, Joint Inquiry Staff

October 1, 2002

INTRODUCTION

Mr. Chairman and members of the Joint Committee, good morning. In prior hearings, we have discussed specific information sharing issues relating to the performance of the Intelligence Community prior to the events of September 11. Today, I will discuss what our review has uncovered regarding the more systemic aspects of information sharing between the agencies of the Intelligence Community, and between those agencies and other federal, state, and local entities. Before addressing the issue of information sharing, I would, however, like to summarize our review of what the non-Intelligence Community agencies knew about the hijackers.

The Hijackers

We have not found any evidence that non-Intelligence Community agencies had any information prior to September 11 that the 19 individuals who took part in the September 11 attacks had terrorist ties. We also found that the non-Intelligence Community agencies were focused on specific threats to their areas of responsibility, such as airline hijackings or an individual terrorist crossing the border. We did not find any significant focus on a "war" against Bin Ladin, in which terrorist operatives might launch multiple attacks against the continental United States using airplanes as weapons. While the FAA, Customs, State, and INS each had data concerning the 19 hijackers, that data was not related to their terrorist activities or associations. As a result, none of this information would, by itself, have aroused suspicions regarding a planned terrorist attack within the United States. Instead, these agencies had routine information concerning the vital statistics, travel, immigration, and medical status of some of the hijackers.

Prior to September 11th, the FAA had airman records on hijackers Marwan Alshehhi, Mohamed Atta, Hani Hanjour, and Ziad Jarrah. Mohamed Atta filled out a medical history form on July 24, 2000. Marwan Alshehhi was issued a medical certificate on July 24, 2000. A medical record concerning Hani Hanjour dated back to 1996, while a medical record for Ziad Jarrah was issued on July 11, 2000. While the

FAA had some records relating to Zacarias Moussaoui, it could not find any evidence that Moussaoui was ever issued a recreational pilot or higher-level airman certificate.

The INS also had records concerning the 19 hijackers—specifically the type of visa and the duration of the stay adjudicated by the immigration officer for each individual. INS records show that three of the 19, Satam Al Suqami, Nawaf Al Hazmi, and Hani Hanjour had overstayed their visas. According to the INS, Mohamed Atta filed an application to change his visa status from B-1 to M-1, and this was granted on July 17, 2001. The B-1 visa is issued to foreign nationals for personal travel to the United States while the M-1 visa is issued to foreign nationals to study in the United States. However, on July 19, 2001, Mr. Atta was admitted to the United States based on his then current B-1 visitor visa.

U.S. Customs Service officials advised the staff that the only information Customs had concerning the 19 hijackers prior to September 11 was contained in the routine forms they filled out when they arrived in the United States.

Information Sharing Obstacles to Counterterrorism

The Joint Inquiry Staff interviewed numerous Intelligence Community officials and officials of departments and agencies outside the Intelligence Community to determine the extent to which terrorist-related information flows as necessary to avert terrorist attacks. The staff also reviewed relevant documents at the Departments of State, Treasury, Defense, Transportation, and Energy and at the U.S. Customs Service and the Immigration and Naturalization Service (INS), focusing on information received from the Intelligence Community.

Our review also included what the agencies outside the Intelligence Community knew about the hijackers before September 11 and the specific information on which that knowledge was based. The staff reviewed visa and immigration information, and also

what had been shared with these agencies regarding threats to U.S. landmarks using aircraft as weapons, and terrorist financing in the United States. The staff also interviewed various officials in Department Of Defense agencies and components, and in the military services, regarding the support they provided to or received from, the Intelligence Community agencies.

In February 2001, Director of Central Intelligence (DCI) George Tenet publicly testified to Congress that "the threat from terrorism is real, it is immediate, and it is evolving." Furthermore, "[Osama] bin Ladin and his global network of lieutenants and associates remain the most immediate and serious threat." The events of September 11, 2001, in retrospect, underscore the significance of the DCI's concerns. Our work to date indicates that the flow of information between all agencies did not necessarily keep pace with the increasing nature of the threat.

During the course of our interviews, intelligence and non-intelligence personnel alike complain that a range of political, cultural, jurisdictional, legal, and bureaucratic issues are ever-present hurdles to information sharing. Prior to the passage of the USA Patriot Act, many suggested that law enforcement information was not adequately shared with the Intelligence Community. The reverse was also apparently true despite amendments to the National Security Act in the 1990s designed to make clear that foreign intelligence could be collected for, and shared with, U.S. law enforcement agencies.

We were also told that not all threat information in possession of the Intelligence Community or law enforcement agencies is shared with agencies that need it the most in order to counter the threats. For example, the FAA was not provided a copy of the FBI's Phoenix memorandum prior to September 11, 2001 and still did not have a copy two weeks after the matter had become public in early 2002. In another example, the CIA did not provide the Department of State with a large number of intelligence reports that included the names of terrorist suspects until shortly after September 11, 2001. The reasons for this reluctance to share range from a legitimate concern about the protection

of intelligence sources and methods to a lack of understanding of the functions of other agencies.

The vast majority of the information related to the hijackers or to threats posed by aircraft came to the non-Intelligence Community agencies from the CIA, NSA, and FBI. According to officials from the Departments of Transportation, State, Energy, Defense, and Treasury, unless information in the possession of the CIA, NSA, and FBI is shared on a timely basis, they are unable to include dangerous individuals on various watch lists to either deny them entry into the United States or apprehend suspected terrorists in the United States. The State Department, the Immigration and Naturalization Service (INS) and the U.S. Customs Service all maintain watchlists of named individuals. The Federal Aviation Administration (FAA), Drug Enforcement Administration (DEA), INS, and other agencies also perform a limited amount of information collection designed to place individuals on watchlists.

The staff review, to date, has found no single agency or database or computer network that integrates all counter terrorism information nationwide. Information about the hijackers and al-Qa'ida can be found in disparate databases spread among a range of intelligence and civilian agencies. Specifically, as exemplified by the Phoenix communication that was discussed in detail at a prior hearing, FBI information related to possible al-Qa'ida terrorists was scattered in various regional offices and not shared with the FBI headquarters or other agencies. Furthermore, law enforcement, immigration, visa, and intelligence information related to the 19 hijackers was not organized in any manner to allow for any one agency to detect terrorism-related trends and patterns in their activities.

Numerous officials state that there are many hurdles to sharing information. A major issue relates to the availability of properly cleared personnel. Federal officials told us that clearing a person for access to Sensitive Compartmented Intelligence (SCI) takes anywhere from one year to a year and a half and describe the process as cumbersome and unwieldy. However, without SCI clearances, non-intelligence community agencies are

often unable to access vital counterterrorism-related information. Some federal agencies we visited which did not have personnel cleared for SCI data, advised that they could have benefited from receiving more specific data on potential terrorists. We were also told that many state and local agencies do not have personnel cleared for even the lowest level of access to national security information, let alone SCI access. As a result, while appropriately cleared FAA, TSA, INS, and Department of State officials may receive significant intelligence information, they may be unable to disseminate data within their organization or to state and local officials because the potential recipients are not cleared to receive it.

Another difficulty mentioned repeatedly is the "originator control" or ORCON caveat. Agencies that generate intelligence impose this caveat when disseminating raw and finished intelligence to prohibit further dissemination without their approval. Thus, an agency may receive very important information that could be of use to a third agency that is not a recipient, but may be unable to share it because of the caveat. Although this matter can be resolved through agreed-upon procedures, the process can be lengthy and cumbersome and may not meet the near-real time lines often required to track and apprehend terrorist suspects.

We were told that because information sharing is inconsistent and haphazard, agencies have tried various means available to them to circumvent the hurdles. These include: (1) signed memoranda of agreements with other agencies, (2) the use of detailed employees to other intelligence and law enforcement agencies; (3) participation in joint task forces; and (4) attempts to design and field common databases.

Agencies Detail Employees Try To Ensure Access To Intelligence Information

One method of dealing with information sharing issues is for agencies to detail employees to CIA, NSA, FBI, and other agencies in an attempt to improve access to relevant information on a timely basis. Theoretically, at least, the agencies believe this is one of the most effective ways to access a greater amount of information from the Intelligence Community. Thus, the Departments of State, Transportation, Treasury, and Energy and the INS, Customs, and other organizations have utilized detailees at the DCI's Counterterrorist Center (CTC), at the FBI, and, to a lesser extent, at the NSA. In turn, Intelligence Community agencies also send detailees to the non-intelligence agencies and law enforcement agencies. Numerous task forces and cooperative agreements exist between the DOJ's FBI and border security and intelligence agencies.

Although sending employees to another agency has merits, it is an imperfect response to the problem. The JIS was told repeatedly that detailees are not afforded the same access to information as host agency employees. The almost unanimous opinion among the detailing agencies is that host agencies still restrict access to information and limit the databases that can be queried by detailees from other agencies on grounds of personnel or information security, and intelligence policies. We were told that detailees are often advised about the existence of intelligence after an ad hoc judgment to share the information is made by host agency employees. Representatives of the detailing agencies advised that host agency employees may not have the proper understanding of the issues that are of interest to other agencies and consequently provide detailees with information that often lacks proper context. Representatives of the detailing agencies also suggested that success in gaining access to information can be personality driven. All agencies recognized that agency to agency open and secure access through electronic means would be the optimal solution answer whereas the detailing of employees is basically a value-added approach.

Joint Terrorism Task Forces

To improve information sharing, the DOJ, through the FBI, has established 56 Joint Terrorism Task Forces (JTTFs) to involve other federal, state, and local agencies in investigation of terrorist events. The JTTF program is intended to prevent acts of terrorism before they occur by assisting in identification, investigations, and prosecution. Each JTTF is responsible for dealing with domestic and international terrorism matters within the jurisdiction of the local FBI field office. Agencies participating in the JTTF are required to enter a formal memorandum of understanding that identifies the objectives of the JTTF as both reactive and proactive. In its reactive mission, the JTTF responds to and investigates terrorist incidents. In its proactive mission, the JTTF investigates domestic and foreign terrorist groups and individuals targeting or operating within its jurisdiction with the goal of preventing terrorist events.

The JTTFs are described as an important force multiplier for an FBI field office. The personnel who work at a JTTF serve as, and are treated like, FBI special agents. They are given cases to investigate and access to most of the field office's information systems. In the New York field office, however, JTTF personnel told the staff that non-FBI personnel are prevented in some cases from having access to the FBI's information systems. The result is that non-FBI members must rely on FBI special agents to obtain information that will assist them in their investigations.

The non-FBI members' knowledge, experience and affiliations with state and local law enforcement organizations serve to enhance the ability of the JTTF to deal with terrorism. In this regard, we were told the most highly lauded member of the JTTF is often the INS. INS membership in the JTTF repeatedly has allowed the FBI personnel in the New York, Boston, and Phoenix field offices to use violations of the immigration laws to disrupt and obtain information from individuals the FBI suspects of being terrorists or of having terrorist connections. The INS-FBI collaboration has been instrumental in getting relevant information from these individuals.

The staff was told that, a consistent complaint against the JTTF program has been the lack of participation by local law enforcement organizations. While these organizations are often viewed as not being interested in participating in the JTTF, their absence leaves a void in the JTTF. For their part, local law enforcement organizations assert that by participating in the JTTF program they lose officers, to work on what are largely considered " FBI issues", who would otherwise be patrolling their cities' neighborhoods. Another complaint from JTTF participants is that, prior to September 11th, individuals who were assigned to the JTTF were not always the best for the job. We were told that some law enforcement organizations reportedly viewed the JTTF as a way of getting rid of "deadwood and working retired." This trend changed dramatically after September 11th, we are told.

FAA/TSA

Following the hijacking of a TWA aircraft in the Middle East in the mid 1980s the FAA established a small office (now a part of the Transportation Security Administration) to review the incoming intelligence regarding threats to aviation. The intelligence is translated into information circulars, emergency amendments and security directives for the aviation industry. The circulars and directives are issued to domestic and foreign airlines and to the airports to advise them of current and potential terrorist threats. They are also provided to the Intelligence Community and law enforcement agencies.

Prior to September 11, the FAA had issued a number of circulars and directives as a direct result of intelligence received from the Intelligence Community regarding extremist Islamic groups. These FAA publications advised the airlines of the methods that might be used by such groups to hijack an airplane or to plant explosives in airplanes. None, however, have been found that discussed crashing planes into buildings.

The Intelligence Community is required by law to provide the Department of Transportation (DOT) with intelligence concerning international terrorism. As a result, the Department receives intelligence from the CIA, the Department of State, FBI, NSA, and DIA. However, DOT officials advise the staff that they do not believe they receive all the available intelligence that is needed to perform their mission. In their view, the agencies that collect the information make decisions on what is relevant for, and what should be shared with, the DOT. The issue reportedly is one of context and depth of understanding. By not receiving the sum total of the intelligence on all transportation issues, the TSA may not be able to connect events or to link suspicious activities. Finally, TSA officials stated that, although they can submit their requirements to the Intelligence Community through established procedures, there is nothing that requires the Intelligence Community to collect against those requirements.

Although no indications have been found that the FAA knew of the terrorist connections of the hijackers, the FAA did have detailed information regarding those who were pilots. The FAA maintains records of all certificated airman—those who possess a U.S.-issued certificate, and also on all U.S. registered aircraft. According to the FAA, there are over one million airmen files, of which approximately 626,000 are pilots. Representatives of the FAA stated that the airmen file remains open until receipt of a death certificate. Each certificate contains specific medical information, flight test results, score, engine ratings, incident history, and enforcement activity. These records are kept in Oklahoma City, Oklahoma by the Department of Transportation—specifically the FAA Civil Aviation Registry—and are available to all federal, state and local law enforcement agencies.

According to TSA, shortly after Zacarias Moussaoui's arrest, the FBI contacted it and asked for information on him from the airman records. FAA personnel in Minneapolis advised the FBI to contact the FAA office in Chicago and that office put the FBI in touch with the Oklahoma City center. TSA officials in Washington, D.C. told the staff that they were puzzled that the FBI did not contact the Oklahoma center directly since it was designed to support law enforcement.

Immigration and Naturalization Service

The Immigration and Naturalization Service (INS) maintains records on all visitors who arrive in the United States. INS officials told the staff that the Law Enforcement Support Center (LESC) in Burlington, Vermont is a key data-sharing center designed to support other law enforcement agencies. The LESC assists in determining the status of detainees or to find persons. INS officials stated that the August 2001 notice to watchlist Nawaf al Hazmi and Kahlid al Mihdhar was not accompanied by any specific notation that indicated that the INS should use all means possible to find these two suspects. INS officials said that, had they been told to put the highest priority on that search, they would have used the LESC and might have found the two suspects prior to September 11, 2001.

Defense Intelligence Agency

The Director of DIA chairs a standing committee that serves as an integrating mechanisms for the DOD: the Military Intelligence Board (MIB). DCI representatives usually attend and participate in its discussions. Over time, the MIB has wrestled with information sharing issues prior to September 11. According to the DIA, information-sharing issues such as restrictive caveats (e.g., originator or "ORCON" controlled information), handling of information in virtual and collaborative workspaces, limited distribution to senior officials only, and support to homeland defense have been discussed by the MIB since at least the mid-1990's. While most of the specific discussion at MIB meetings is classified, there are enough unclassified examples to provide some definition of the range of information sharing topics addressed. For example, the need to establish an information sharing mechanism was addressed at least as early as February 1995 in the context of multi-agency operations in Haiti. Several additional examples follow, drawn from the records of the proceedings of the group.

In September 1998, an MIB was convened to receive briefings on the East African Embassy Bombings and the War on Terrorism. Generally recognizing the need for broad sharing of information in that context, one Command representative observed that there must be a "domestic piece", referring to FBI reporting. Another representative stressed that there was a "commercial piece" as well, with the FAA. Yet a third representative encouraged intra-organizational information sharing as it had done within its organization. Finally, another Command supported breaking through the existing information restriction barriers and recommended a collaborative strategy regarding how to examine and attack terrorist organizations. It is not clear whether any follow-up actions were taken as a result of this discussion.

In April 1999, the MIB met to receive a briefing on computer network defense. Challenges to both network defense and information sharing were listed as: law enforcement vs. public interests; the interagency process; and policy and legal issues

In January 2000, the MIB met for a briefing concerning a DIA asymmetric warfare initiative. Both the NSA and the Coast Guard representatives spoke to the legal complications of the portion of the concept that pertained to homeland defense. During a July 2000 update, NSA reiterated its concern about policy and legal issues, especially regarding NSA collection in support of homeland defense and terrorism. The Coast Guard cautioned that new environments and new threats might mean old rules could no longer apply. Again it is not yet apparent whether this discussion of obstacles to real information sharing needs led to further action.

In October 2000, the MIB discussed the issue of "need to know." A DCI Community Management staff representative said the CIA was working to resolve the issue in connection with information architectures that would allow analysts to share information. A DIA attendee said that philosophically, defense intelligence had moved away from "need to know," but that CIA still adhered to the principle "as a foundation." The DIA attendee concluded that the defense intelligence community would not be able to bridge the gap with CIA on this information sharing issue.

Senior DIA officials told the staff that information-sharing issues are not new to the Intelligence Community and are not limited to the context of September 11. According to them, the basic legal, community, cultural, and technological barriers have been understood for years. After the USS Cole attack, the DIA reportedly took significant steps to alter its structure, processes, products, and policies associated with terrorism analysis. DIA officials advised that the DIA now challenges its analysts to "think out of the box" and exploit all relevant information, including open source reporting. They also stated that DIA has implemented mechanisms that allow more effective receipt and dissemination of critical intelligence information.

The DIA has established a Joint Intelligence Task Force for Combating Terrorism (JITF-CT) to help enhance terrorist threat warning and analysis capabilities and significantly enhance communications and sharing between DIA, the FBI, and CIA. Deputy Secretary of Defense Paul Wolfowitz identified the value of the JITF-CT during his testimony to the Joint Inquiry on September 19, 2002. He also identified the issue of information discovery where "many agencies collect intelligence and lots of agencies analyze intelligence, but no one is responsible for the bridge between collection and analysis." Finally, Mr. Wolfowitz questioned the current culture that discourages collaboration and criticized the lack of sharing of information that leads to forfeiting of U.S. technological advantages.

According to DIA personnel, there have been mixed results with these Intelligence Community partnerships, i.e., the mere act of assigning an analyst to another organization does not ensure a greater level of access to information or more open sharing of information. DIA acknowledged that its analysts who are detailed to counterpart organizations do not have unfettered and unconditional access to all relevant terrorist information. Former DIA Director Admiral Thomas Wilson explained to the staff that "information sharing" implies that one "owns the information." He did not agree with that concept. According to Wilson, agencies need to change their culture and shed the belief that they own the information—the information belongs to the United States Government and the entire Intelligence Community.

Department of Treasury

Several Treasury Department components receive intelligence relating to financial matters from the CIA, NSA, FBI and other intelligence agencies. The JIS interviewed Treasury officials at the Financial Crimes Enforcement Network (FinCEN), the Office of the Financial Assets Control (OFAC), the Secret Service, and US Customs.

Officials in Treasury's Financial Crimes Enforcement Network (FinCEN) and the U.S. Customs Service reported to the staff that they submit intelligence requirements to the Intelligence Community, but have no assurances that the intelligence will be collected and provided to them on a timely and regular basis.

The Secret Service at Treasury occupies a unique position because of its primary mission to protect the President of the United States. According to the Secret Service, it receives the intelligence that is necessary for it to perform that particular mission. It also reportedly receives all relevant intelligence regarding the maintenance of the protective perimeter around the White House.

Post-September 11, U.S. Customs officials used information available in Treasury databases to develop a comprehensive analysis of the travel, finances, and linkages of the hijackers. Specifically, U.S. Customs Service analysts used Suspicious Activity Reports (SARs), Currency or Monetary Instrument Reports (CMIRs), and Current Transaction Reports (CTRs) obtained from the Treasury Department. Much of the analysis was completed by November 2001.

Customs officials advised that the majority of the information used in that analysis to show the domestic and international activities and associations of the hijackers came from law enforcement databases—specifically the Inter-agency Border Inspection System (IBIS)—and not intelligence. IBIS is a major information-sharing system that connects Customs with INS, the Department of State, FBI, National Law Enforcement

Telecommunications System (NLETS), Drug Enforcement Agency (DEA), Alcohol, Tobacco, and Firearms (ATF), Secret Service, Internal Revenue Service (IRS), FAA, and the Royal Canadian Mounted Police. According to the Customs service, there are over 30,000 users of IBIS, but it has no connection to the Intelligence Community. Customs officials told the staff that they need to have regular and consistent information from the Intelligence Community on terrorism related matters.

Department Of State

As mentioned earlier, and explained in more detail in the September 18, 2002 JIS staff statement, State Department officials advised the staff that at least 1,500 CIA Central Intelligence Reports (CIRs) containing terrorist names were not provided to the TIPOFF watchlisting program until after September 11, 2001. After an analysis of those CIRs was completed, the names of approximately 150 suspected terrorists were identified and 58 new suspected terrorist names were added to the TIPOFF watchlist. This lapse in sharing intelligence, and the failure to add the names of at least two of the hijackers to the State watchlist prior to September 11, were attributed to a lack both of resources and of awareness of watchlisting. State Department officials advised that they have had continuing difficulty obtaining data for watchlisting purposes from the National Crime Information Center's Interstate Identification Index (NCIC III) that is managed by the FBI.

Foreign Terrorist Tracking Task Force

The Attorney General established the Foreign Terrorist Tracking Task Force (FTTTF) in October 2001 at the request of the President. The FTTTF's mission is to assist in keeping foreign terrorists and their supporters out of the United States by developing information through "data-mining" technologies and providing that information to law enforcement and other operational agencies. The FTTTF relies on

public, government, and other databases to link relevant information about terrorists and their supporters.

According to FTTTF officials, it is attempting to solve the problem of identifying possible terrorist suspects. The FTTTF is intended to co-locate data from the law enforcement and intelligence communities, and other government and non-government sources and, then, provide that information to federal, state, and local operational agencies.

FTTTF officials state that they are encouraged that the databases and interagency participation in the program have been progressing as envisioned. The FTTTF is not a separate agency, it is a multi-agency task force that is entirely staffed with detailees from different agencies. The Department of Defense's Joint Counterintelligence Assessment Group provides primary technical support to FTTTF.

FTTTF officials reported that several thousand individuals from several countries have been already identified as "abscondees" within the United States by the FTTTF. Many new addresses for "cold" abscondees were provided to the INS and the INS is now working closely with the FTTTF to identify individuals who are engaged in immigration law violations. Additionally, the FTTTF works closely with the FBI on the identification and location of terrorists and their supporters.

Executive And Congressional Recognition Of Information Sharing Issue

The events of September 11, 2001 have led to an almost universal acknowledgement in the United States Government of the need for consolidating and streamlining collection, analysis, and dissemination of information concerning threats to the United States and its interests. According to the President's National Strategy for Homeland Security ("the Strategy"), intelligence contributes to every aspect of homeland

security and is a vital foundation for the homeland security effort. The Strategy recognizes that U.S. information technology is the most advanced in the world, but that our information systems have not adequately supported the homeland security mission. According to the Strategy, the U.S. government spends about $50 billion per year on information technology, but the systems purchased are not compatible between the agencies of the federal government, or with state and local entities. The Strategy also acknowledges that legal and cultural barriers often prevent agencies from exchanging and integrating intelligence and other information.

In response to these problems, the Strategy first calls for integrating information sharing across the federal government through the Critical Infrastructure Assurance Office (CIAO). Under this plan, the CIAO would design and implement an interagency information architecture to support efforts to find, track, and respond to terrorist threats. The CIAO would coordinate groups focusing on border and transportation security and other countermeasures to the use of weapons of mass destruction. As part of this effort, the FBI will create a consolidated Terrorism Watch List that includes information from both intelligence and law enforcement sources.

The Strategy also calls for integrating information sharing across state and local governments, private industry, and among the U.S. citizenry. Using modern information technology, more information is to be shared among various databases. The FBI and other agencies will augment information that currently is available in the National Crime Information Center databases and National Law Enforcement Telecommunications Systems. This information integration effort will require that Intelligence Community agencies make efforts to remove classified information from some documents in order to allow them to be shared with state and local officials.

Finally, the Strategy calls for the adoption of standards for information that is in electronic form and is relevant to homeland security. According to the Strategy, terrorist-related information from the databases of all government agencies with responsibilities for homeland security is to be integrated. The Department of Justice, FBI, and other

federal agencies, and numerous state and local law enforcement agencies, will then be able to use data-mining tools to apply this information to the homeland security mission.

Major provisions of two of the homeland security-related bills now pending before Congress would promote the sharing of critical homeland security information regarding threats between federal intelligence agencies and law enforcement agencies as well as state and local officials, sheriffs, governors, mayors, other elected officials, and other emergency responders. The bills recognize the continuing need to protect sensitive sources and collection methods by granting security clearances to appropriate state and local personnel.

The bills would also direct the President to develop procedures by which federal agencies will share homeland security information with, and receive such information from state and local personnel. Further, the bills would require information sharing systems to have the capability to transmit classified or unclassified information, have the capability to restrict delivery of information based on the recipient's need to know, and be accessible to appropriate state and local personnel.

In recent years, a number of Commissions established by the Congress have reported on the ability of the United States to respond to terrorist events and have recommended that steps be taken to encourage closer cooperation between the intelligence and law enforcement communities. The hearings of this Joint Inquiry have shown that, although there is no information to indicate with certainty that the terrorist attacks of September 11, 2001 could have been prevented, some have suggested that certain terrorist acts may have been facilitated by continuing poor information exchanges between intelligence and law enforcement agencies and by blurred lines of organizational responsibility.

One of the mechanisms established by Congress, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, looked very closely at the issues relating to the sharing of counter terrorism intelligence

with state and local officials. The Advisory Panel was established by the National Defense Authorization Act for Fiscal Year 1999, and was chaired by then-Governor James Gilmore of Virginia who will be appearing as a witness today. The Advisory Panel issued three reports in December 1999, 2000, and 2001.

In its first report, the Advisory Panel reported that state and local officials had expressed a need for more intelligence, and for better information sharing among entities at all levels regarding potential terrorist threats. The report stated that, while the Panel was acutely aware of the need to protect classified national security information and the sources and methods by which it may have been obtained, it believed more could be done to provide timely information up, down, and laterally, at all levels of government to those who need the information to provide effective deterrence, interdiction, protection, and response to potential threats.

The Panel's second annual report stated that the potential connection between terrorism originating outside the United States and terrorist acts perpetrated inside the United States means that "foreign" terrorism may not be easily distinguished from "domestic" terrorism. The report urged that an even more comprehensive dissemination system than the JTTFs must be developed to provide information through expanded law enforcement channels for further dissemination to local response entities. In its third and final report, the Panel described the results of a survey it had commissioned that substantiated the panel's view that state and local entities are in need of threat assessments and better intelligence concerning potential terrorist activities.

The premise of the Panel throughout its work has been that all terrorist incidents are local, or at least will begin that way. The Panel recommended that a federal office for combating terrorism establish a system for providing clearances to state and local officials and that the FBI implement an analytic concept similar to the CIA's "Reports Officers" to do a better job of tracking and analyzing terrorism indicators and warnings.

GAO's Assessment Of Information Sharing
Within And Between Federal, State, And Local Agencies

The General Accounting Office has completed a number of reports for Congress that focus on combating terrorism, information sharing, and homeland security. In addition, GAO's written statement for the record for this hearing emphasizes the need for a commitment by the leadership of the FBI, CIA, and other agencies to transform the law enforcement and intelligence communities and achieve the most effective information sharing possible to combat terrorism.

GAO has confirmed that, the FBI, CIA, NSA, and other agencies have distinct organizational cultures. Also, legal walls, classification walls, and historically-ingrained walls of bureaucratic practice exist between these agencies. As GAO views the situation, only with the commitment, effectiveness and persistence of strong and visionary managers, will these walls be brought down and greater amounts of information sharing occur.

The three problems of information sharing identified by GAO as important to resolve if national, state, and local governments are to succeed in their collective war on terrorism include fragmentation, technological impediments, and ineffective collaboration. The GAO's assessment regarding the importance of technological impediments is supported by the FBI's inability to share information among its field offices and headquarters and with other agencies. The problem of information fragmentation is also illustrated by the fact that the intelligence office at the Federal Aviation Administration now at the Transportation Security Administration (TSA)--received information indicating that reputed terrorist bomber Ahmed Ressam had been arrested while trying to enter the United States from Canada with the intent of bombing the Los Angeles International Airport. It then issued an analysis of the bomb equipment seized, but this analysis was not directly shared with the Intelligence Community at the same time that it was released to the airports and the airlines.

Additional Databases

The Joint Inquiry Staff has reviewed numerous databases that contain important financial, travel, and vital statistics information. The Staff also has been informed of other powerful search mechanisms that have not been tapped because agencies are not fully aware of their existence or capabilities.

For example, both INS at the Justice Department and the Diplomatic Security Service (DSS) at the State Department claim that their databases and capabilities were never fully exploited in the FBI's efforts to locate the two hijackers, al Mihdhar and al Hazmi, who were identified by CIA in August 2001 as having entered the United States. Individuals at both INS and DSS claim that they may have been able to locate the two hijackers before September 11, 2001, had they been provided with the full context of the search and all the intelligence that was available on the two hijackers.

The multiple databases that exist with the Intelligence Community cannot be discussed here because of national security classification. However, we can briefly describe some of the many unclassified databases and task forces that exist and are intended to facilitate sharing information among law enforcement agencies.

Selected Law Enforcement Databases

NCIC: The FBI's National Crime Information Center is a national index of theft reports, warrants, and other criminal justice information submitted by law enforcement agencies across the country. NCIC provides real-time notification of information regarding persons and property to police officers and law enforcement officials.

NLETS: NLETS is a nationwide network that links all states and many federal agencies together for the exchange of criminal justice information. In each state, an agency is responsible for maintaining in-state law enforcement telecommunication systems that deliver messages throughout the state. Each state's criminal justice system can access any other state's criminal justice system to obtain a variety of information, including vehicle registration, drivers license, and criminal history records. Other data includes plane, boat, and gun registrations.

TIPS: Terrorism Information and Prevention System, established by the FBI consists of a website and a toll free 800 number for reports of any information about possible terrorist crimes. The phone tip line received over 180,000 calls in less than two months and generated about 30,000 leads.

CODIS: Established by the FBI in 1990, the Combined DNA Index System is a national index of DNA profiles. It is a key tool for solving violent crimes by enabling federal, state, and local crime labs to exchange and compare DNA profiles electronically, thereby linking crimes to each other and to convicted offenders.

NIBIN: The National Integrated Ballistics Information Network attempts to unify Bureau of Alcohol, Tobacco, and Firearms and FBI firearms databases.

NDPIX: The National Drug Pointer Index is a system that allows state, local, and federal agencies to determine if a suspect is under investigation by any other participating agency.

TECS: Treasury's Enforcement Communications Systems is a computerized information system designed to identify individuals and businesses suspected of involvement in violations of federal law. TECS is also a communications system permitting message transmittal between Treasury law enforcement offices and other national, state, and local law enforcement agencies. TECS provides access to the FBI's National Crime Information Center (NCIC) and the National Law Enforcement

Telecommunication Systems (NLETS, with the capability of communicating directly with state and local enforcement agencies.

IBIS: The Interagency Border Inspection System assists border enforcement agencies in focusing their limited resources on potential non-compliant travelers at ports of entry. IBIS provides the law enforcement community with access to computer-based enforcement files of common interest. It also provides access to the FBI's National Crime Information Center (NCIC) and allows its users to interface with all fifty states via the National Law Enforcement Telecommunications Systems (NLETS). IBIS resides on the Treasury Enforcement Communications System (TECS) at the Customs Data Center. IBIS also contains the INS' NAILS database. An IBIS network with more than 24,000 computer terminals provides field-level access. These terminals are located at air, land, and sea ports of entry. IBIS keeps track of information on suspect individuals, businesses, vehicles, aircraft, and vessels. IBIS terminals can also be used to access NCIC records on wanted persons, stolen vehicles, vessels or firearms, license information, criminal histories, and previous Federal inspections. The information is used to assist law enforcement and regulatory personnel.

NAILS: The National Automated Immigration Lookout System is a central mainframe computer system that provides a reliable method of verifying the admissibility of an individual and preventing inadmissible individuals from entering the United States. NAILS facilitates inspection and investigation processes by providing quick and easy retrieval of biographical or case data on individuals who should not be permitted to enter the United States. Individual INS applications supply the data contained in NAILS II. Other information is provided by Federal, state, local, and foreign government agencies, and other entities.

SELECTED FEDERAL TASK FORCES

JTTF: Prior to September 11, 2001 there were thirty-four JTTFs nationwide that included members from federal agencies such as the U.S. Marshals Service, the U.S.

Department of State's Diplomatic Security Service, the Bureau of Alcohol Tobacco and Firearms, the Immigration and Naturalization Service, the U.S. Secret Service and local entities such as the New York State Police. After September 11, the Department of Justice established 56 JTTFs, one in each FBI field office, to enhance the FBI's ability to promote coordinated terrorism investigations among FBI field offices and law enforcement organizations nationwide. The JTTFs now involve over 3,700 agents, compared to 2,178 before September 11.

ATTF: To integrate and further coordinate antiterrorism activities in the field, the Justice Department created 93 Anti-Terrorism Task Forces, one in each U.S. Attorney's district—to integrate the communications and activities of local, state and federal law enforcement. The ATTFs include a 24 hour, seven day per week, contact system to ensure that key members of the ATTFs and other agencies can quickly communicate and respond to any future terrorist attacks.

FTTTF: The Foreign Terrorist Tracking Task Force was established to better ensure that federal agencies, including the FBI, INS, and Customs Service coordinate their efforts to bar from the United States and locate aliens who are suspected of engaging in terrorist activity, or who provide material support to terrorist activity.

Conclusion

In summary, the Joint Inquiry Staff believes that much information of great potential utility to the counterterrorism effort exists in the files and databases of many federal, state, and local agencies, as well as in the private sector. However, that information is not always shared or made available in timely and effective ways to those who are in a position to act upon it, add it to their analysis, and use it to better accomplish their individual missions. Our review found problems in maximizing the flow of relevant information both within the Intelligence Community as well as to and from those outside the Community. The reasons for these information disconnects can be, depending on the

case, cultural, organizational, human, or technological. Comprehensive solutions, while perhaps difficult and costly, must be developed and implemented if we are to maximize our potential for success in the war against terrorism.

TESTIMONY OF ELEANOR HILL, STAFF DIRECTOR, JOINT INQUIRY STAFF

Ms. HILL. Thank you Mr. Chairman. Good morning, Mr. Chairman and members of the Joint Committee. In prior hearings, we have, as you know, discussed very specific information sharing issues relating to the performance of the Intelligence Committee prior to the events of September 11. Today, I will discuss what our review has, to date, uncovered regarding more systemic aspects of information sharing between the agencies of the Intelligence Community and between those agencies and other Federal, State and local entities. Before addressing the issue of information sharing, however, I would like to first summarize our review of what we have found the non-intelligence community agencies knew about the hijackers.

In short, we have not found any evidence that non-Intelligence Community agencies had any information prior to September 11 that the 19 individuals who took part in the attacks had terrorist ties. We also found that the non-Intelligence Community agencies were, for the most part, focused on specific threats to their areas, their particular areas of responsibility, such as airline hijackings or an individual terrorist crossing the border.

We did not find any significant and sustained focus on a war against bin Ladin in which terrorist operatives might launch multiple attacks against the continental United States using such tactics as airplanes as weapons. While the FAA, the Customs Service, the State Department and INS each had data concerning the 19 hijackers, that data was not related to their terrorist activities or associations. As a result, none of this information would, by itself, have aroused suspicions regarding a planned terrorist attack within the United States. Instead, these agencies had routine information concerning the vital statistics, travel, immigration and medical status of some of the hijackers.

For example, prior to September 11, the FAA had airman records on hijackers Marwan Alshehhi, Mohamed Atta, Hani Hanjour and Ziad Jarrah. The INS also had records concerning the 19 hijackers, specifically the type of visa and the duration of the stay adjudicated by the immigration officer for each individual.

Finally, U.S. Customs Service officials have advised the staff that the information Customs had concerning the 19 hijackers prior to September 11 was contained in the routine forms that they filled out when they arrived in the United States. Moving on to the general topic of information sharing, during the course of our interviews, intelligence and non-intelligence personnel alike complained that a range of political, cultural, jurisdictional, legal and bureaucratic issues are ever-present hurdles.

Prior to the passage of the USA PATRIOT Act, many suggested that law enforcement information was not adequately shared with the Intelligence Community. The reverse was also apparently true despite amendments to the National Security Act in the 1990s which were designed to make clear that foreign intelligence could be collected for and shared with U.S. law enforcement agencies.

We were told that not all threat information in possession of the Intelligence Community or law enforcement agencies is necessarily shared with agencies that need it the most in order to counter the

threats. For example, the FAA was not provided a copy of the FBI's Phoenix memorandum prior to September 11, 2001, and still did not have a copy two weeks after the matter had become public in early 2002.

In another example, the CIA did not provide the Department of State with large numbers of intelligence reports that included the names of terrorist suspects until shortly after September 11, 2001. The reasons for this reluctance to share ranged from a legitimate concern about the protection of intelligence sources and methods to a lack of understanding of the functions of other agencies. The vast majority of the information related to the hijackers, or to threats posed by aircraft, came to the non-Intelligence Community agencies from the CIA, the National Security Agency and the FBI. According to officials from the Departments of Transportation, State, Energy, Defense and Treasury, unless information in the possession of FBI and CIA is shared on a timely basis, they are unable to include dangerous individuals on various watchlists to either deny them entry into the United States or apprehend suspected terrorists while in the United States.

The State Department, the Immigration and Naturalization Service, and the U.S. Customs Service all maintain watchlists of named individuals. The Federal Aviation Administration, the Drug Enforcement Administration, INS and other agencies also perform a limited amount of information collection designed to place individuals on watch lists.

The staff review to date has found no single agency or database or computer network that integrates all counterterrorism information nationwide. Information about the hijackers and about al-Qa'ida can be found in disparate databases spread among a range of intelligence and civilian agencies. Specifically, as exemplified by the Phoenix communication, FBI information related to possible al-Qa'ida terrorists was often scattered in various regional offices and not shared with the FBI headquarters or with other agencies.

Furthermore, law enforcement, immigration, visa and intelligence information related to the 19 hijackers was not organized in any manner to allow for any one agency to detect terrorism-related trends and patterns in their activities. Numerous officials stated that there are many hurdles to sharing information. A major issue for example, relates to the availability of properly cleared personnel. Some Federal agencies we visited, which did not have personnel cleared for sensitive compartmented information, or SCI data, advised that they could have benefitted from receiving more specific data on potential terrorists.

We were also told that many State and local agencies do not have personnel cleared for even the lowest level of access to national security information, let alone SCI access. As a result, while appropriately cleared, FAA, TSA, INS and Department of State officials may receive significant intelligence information, they may be unable to disseminate data within their organization or to State and local officials because the potential recipients are not cleared to receive it.

Another difficulty mentioned repeatedly is the originator control, or ORCON caveat. Agencies that generate intelligence impose this caveat when disseminating raw and finished intelligence to pro-

hibit further dissemination without their approval. Thus, an agency may receive very important information that could be of use to a third agency that is not a recipient, but may be unable to share it because of the caveat. Although this matter can be resolved through agreed-upon procedures, the process can be lengthy and cumbersome, and may not meet the near real-time lines often required to track and apprehend terrorist suspects.

We were told that because information sharing is inconsistent and haphazard, agencies have tried various means available to them to circumvent the hurdles. These include signed memorandums of agreement with other agencies, the use of detailed employees to other intelligence and law enforcement agencies, participation in joint task forces, and attempts to design and field common databases.

I want to, at this point, just briefly go through what a number of different agencies told us during our staff discussions with them, and I will start with the FAA and the Transportation Security Administration. Following the hijacking of a TWA aircraft in the Middle East in the mid-1980s, the FAA established a small office, which is now a part of the Transportation Security Administration, to review the incoming intelligence regarding threats to aviation. The intelligence is translated into information circulars, emergency amendments and security directives for the aviation industry.

The circulars and directives are issued to domestic and foreign airlines, and to the airports to advise them of current and potential terrorist threats. They are also provided to the Intelligence Community and law enforcement agencies. Prior to September 11, the FAA had issued a number of circulars and directives as a direct result of intelligence received from the Intelligence Community regarding extremist Islamic groups.

These FAA publications advised the airlines of the methods that might be used by such groups to hijack an airplane or to plant explosives in airplanes. None, however, has been found that discussed crashing planes into buildings. The Intelligence Community is required by law to provide the Department of Transportation with intelligence concerning international terrorism.

As a result, the Department receives intelligence from the CIA, the Department of State, the FBI, the NSA and DIA. However, transportation officials advised the staff that they do not believe that they receive all the available intelligence that is needed to perform their mission. In their view, the agencies that collect the information make decisions on what is relevant for and what should be shared with the Department of Transportation. The issue reportedly is one of context and depth of understanding. By not receiving the sum total of the intelligence on all transportation issues, the Transportation Security Administration may not be able to connect events or to link suspicious activities.

TSA officials stated that although they can submit their requirements to the Intelligence Community through established procedures, there is nothing that requires the community to collect against those requirements.

Turning to the Immigration and Naturalization Service, INS, the INS maintains records on all visitors who arrive in the United States. INS officials told the staff that the Law Enforcement Sup-

port Center, or the LESC, in Burlington, Vermont is a key data-sharing center designed to support other law enforcement agencies. The LESC assists in determining the status of detainees or to find persons.

INS officials stated that the August 2001 notice to watchlist Nawaf al Hazmi and Khalid al Mihdhar was not accompanied by any specific notation that indicated that the INS should use all means possible to find these two suspects. INS officials said that, had they been told to put the highest priority on the search, they would have used the LESC and believed they may have found the two suspects prior to September 11.

The Defense Intelligence Agency: The Director of DIA chairs a standing committee that serves as an integrating mechanism for the Department of Defense. It is called the Military Intelligence Board, or MIB. DCI representatives usually attend and participate in its discussions. Over time, the MIB has wrestled with information-sharing issues prior to September 11. According to DIA representatives, information-sharing issues, such as restrictive caveats, handling of information in virtual and collaborative work spaces, limited distribution to senior officials only and support to homeland defense, have been discussed by the MIB since at least the mid-1990s.

For example, the need to establish an information-sharing mechanism was addressed at least as early as February, 1995, in the context of multi agency operations in Haiti. Senior DIA officials told the staff that information-sharing issues are not new to the Intelligence Community and are not limited to the context of September 11. According to them, the basic legal community cultural and technological barriers have been understood for years.

After the USS *Cole* attack, the DIA reportedly took significant steps to alter its structure, processes and policies associated with terrorism analysis. DIA officials advise that the DIA now challenges its analysts to think out of the box and to exploit all relevant information, including open source reporting. They also stated that DIA has implemented mechanisms that allow more effective receipt and dissemination of critical intelligence information. According to DIA personnel, there have been mixed results with the Intelligence Community partnerships. For example, the mere act of assigning an analyst to another organization does not always ensure a greater level of access to information or more open sharing of information.

DIA acknowledged that its analysts who are detailed to counterpart organizations do not have unfettered and unconditional access to all relevant terrorist information. Former DIA Director Admiral Thomas Wilson explained to the staff that information sharing implies that one "owns" the information, a concept with which he does not agree. According to Wilson, agencies need to change their culture and shed the belief that they own the information; the information belongs to the United States Government and the entire Intelligence Community, at least in his view.

Turning to the Department of Treasury, several Treasury Department components receive intelligence relating to financial matters from the CIA, the NSA, the FBI and other intelligence agencies. Officials in Treasury's financial crimes enforcement network

and the U.S. Customs Service reported to the staff that they submit intelligence requirements to the Intelligence Community but have no assurance that the intelligence will be collected and provided to them on a timely and regular basis.

The Secret Service at Treasury does occupy a unique position because of its primary mission to protect the President. According to the Secret Service, it does receive the intelligence that is necessary for it to perform that particular mission. Post September 11, U.S. Customs officials used information available in Treasury databases to develop a comprehensive analysis of the travel, finances and linkages of the hijackers.

Specifically, U.S. Customs Service analysts used suspicious activity reports, currency or monetary instrument reports and currency transaction reports obtained from the Treasury Department. Much of the analysis was completed by November, 2001. Customs officials advised that the majority of the information used in that analysis to show the domestic and international activities and associations of the hijackers came from law enforcement databases, specifically the Interagency Border Inspection System, or IBIS, and not from intelligence. According to the Customs Service, there are over 30,000 users of IBIS, but it has no formal connection apart from the FBI's participation to the Intelligence Community.

Turning to the Department of State, State Department officials advised the staff that at least 1,500 CIRs, Central Intelligence reports, containing terrorist names, were not provided to the TIPOFF watchlisting program until after September 11, 2001.

After an analysis of those CIRs was completed, the names of approximately 150 suspected terrorists were identified and 58 new suspected terrorist names were added to the TIPOFF watchlist. State Department officials advised that they have had continuing difficulty obtaining data for watchlisting purposes from the national crime information centers interstate identification index that is managed by the FBI. The events of September 11, 2001, have led to an almost universal acknowledgment in the U.S. Government of the need for consolidating and streamlining collection, analysis and dissemination of information concerning threats to the United States and its interests.

According to the President's national strategy for homeland security, intelligence contributes to every aspect of homeland security and is a vital foundation for the homeland security effort. The strategy recognizes that U.S. information technology is the most advanced in the world, but that our information systems have not adequately supported the homeland security mission.

According to the strategy, the U.S. Government spends about $50 billion per year on information technology, but the systems purchased are not compatible between the agencies of the Federal Government or with State and local entities. The strategy acknowledges that legal and cultural barriers often prevent agencies from exchanging and integrating intelligence and other information.

In response to these problems, the strategy first calls for integrating information-sharing across the Federal Government through the critical infrastructure assurance office. The strategy also calls for integrating information-sharing across State and local governments, private industry and among the U.S. citizenry. Using

modern information technology, more information is to be shared among various databases.

Finally the strategy calls for the adoption of standards for information that is in electronic form and is relevant to homeland security. According to the strategy, terrorist-related information from the databases of all government agencies with responsibilities for homeland security is to be integrated. The Department of Justice, the FBI and other Federal agencies, as well as numerous State and local law enforcement agencies, will then be able to use data-mining tools to apply this information to the homeland security mission.

In recent years, a number of commissions established by the Congress have also reported on the ability of the United States to respond to terrorist events and have recommended that steps be taken to encourage closer cooperation between the intelligence and law enforcement communities. One of the mechanisms established by Congress, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism involving Weapons of Mass Destruction, looked very closely at the issues relating to the sharing of counterterrorism intelligence with State and local officials. The Advisory Panel was established in 1999 and was chaired by then-Governor James Gilmore of Virginia, who will be appearing here as a witness here this morning.

The Advisory Panel issued three reports in 1999, 2000, and 2001. In its first report, the panel reported that State and local officials had expressed the need for more intelligence and for better information-sharing among entities at all levels regarding potential terrorist threats. The reports stated that while the panel was acutely aware of the need to protect classified national security information and the sources and methods by which it may have been obtained, it believed more could be done to provide timely information up, down and laterally at all levels of government to those who need the information to provide effective deterrence, interdiction, protection and response to potential threats.

The panel's second report stated that the potential connection between terrorism originating outside the United States and terrorist acts perpetrated inside the United States means that foreign terrorism may not be easily distinguished from domestic terrorism.

In its third and final report, the panel described the results of a survey it had commissioned that substantiated the view that State and local entities are in need of threat assessments and better intelligence concerning potential terrorist activities. The premise of the panel throughout its work has been that all terrorist incidents are local, or at least will begin that way.

The panel recommended that a Federal office for combating terrorism establish a system for providing clearances to State and local officials and that the FBI implement an analytic concept similar to the CIA's reports officers to do a better job of tracking and analyzing terrorism indicators and warnings.

Finally, the General Accounting Office has also completed a number of reports for Congress that focus on combating terrorism, information-sharing and homeland security. In addition, GAO's written statement for the record for today's hearing emphasizes the need for commitment by the leadership of the FBI, CIA and other

agencies to transform the law enforcement and intelligence communities and achieve the most effective information-sharing possible to combat terrorism.

In summary, the joint inquiry staff believes that much information of great potential utility to the counterterrorism effort already exists in the files and databases of many Federal, State and local agencies, as well as in the private sector.

However, that information is not always shared or made available in timely and effective ways to those who are in a position to act upon it, add it to their analysis and use it to better accomplish their individual missions. Our review has found problems in maximizing the flow of relevant information both within the Intelligence Community as well as to and from those outside the community. The reasons for these information disconnects can be depending on the case, cultural, organizational, human or technological. Comprehensive solutions, while perhaps difficult and costly, must be developed and implemented if we are to maximize our potential for success in the war against terrorism.

Mr. Chairman, that concludes my statement.

Chairman GRAHAM. Thank you, Ms. Hill for another excellent staff presentation.

We will now turn to our panel of distinguished witnesses who were previously introduced. I would like to ask each to take their place at the table. Each of our committees has adopted a supplemental rule of this joint inquiry that all witnesses shall be sworn. So I would ask our witnesses to rise at this time. Anyone else who might be called to testify at this hearing, if they would rise and take the oath also.

[Witnesses sworn.]

Chairman GRAHAM. The full prepared statements of the witnesses will be placed in the record of these proceedings. I will now call on the witnesses to give their oral remarks in the following order. Governor Gilmore, Ambassador Taylor, Mr. Manno, Mr. Greene, Mr. Andre and Commissioner Norris.

[The prepared statement of Mr. Gilmore follows:]

Testimony of
James S. Gilmore, III
Chairman,
Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction

Before the
Joint Hearing of the
U.S. Senate Select Committee on Intelligence
And the
House Permanent Select Committee on Intelligence
On the
Joint Inquiry into the September 11 Attacks

October 1, 2002

Mister Chairmen, Senate Vice Chairman, House Ranking Member, and Members of the Committees, I am honored to be here today. I come before you as the Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Thank you for the opportunity to present the views of the Advisory Panel.

The Advisory Panel was established by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105–261 (H.R. 3616, 105th Congress, 2nd Session) (October 17, 1998). That Act directed the Advisory Panel to accomplish several specific tasks. It said:

The panel shall--

1. assess Federal agency efforts to enhance domestic preparedness for incidents involving weapons of mass destruction;

2. assess the progress of Federal training programs for local emergency responses to incidents involving weapons of mass destruction;
3. assess deficiencies in programs for response to incidents involving weapons of mass destruction, including a review of unfunded communications, equipment, and planning requirements, and the needs of maritime regions;
4. recommend strategies for ensuring effective coordination with respect to Federal agency weapons of mass destruction response efforts, and for ensuring fully effective local response capabilities for weapons of mass destruction incidents; and
5. assess the appropriate roles of State and local government in funding effective local response capabilities.

That Act requires the Advisory Panel to report its findings, conclusions, and recommendations for improving Federal, State, and local domestic emergency preparedness to respond to incidents involving weapons of mass destruction to the President and the Congress at three times during the course of the Advisory Panel's deliberations—on December 15 in 1999, 2000, and 2001.

The Advisory Panel's tenure was extended for two years in accordance with Section 1514 of the National Defense Authorization Act for Fiscal Year 2002 (S. 1358, Public Law 107-107, 107th Congress, First Session), which was signed into law by the President on December 28, 2001. By virtue of that legislation, the panel is now required to submit two additional reports—one on December 15 of this year, and one on December 15, 2003.

Panel Composition

Mr. Chairman, the events of September 11 and its aftermath have changed the lives of Americans for generations to come. But those attacks had special meaning for this Advisory Panel.

This Advisory Panel is unique in one very important way. It is not the typical national "blue ribbon" panel, which in most cases historically have been composed almost exclusively of what I will refer to as "Washington Insiders"—people who have spent most of their professional careers inside the Beltway. This panel has a sprinkling of that kind of experience—a former Member of Congress and Secretary of the Army, a former State Department Ambassador-at-Large for Counterterrorism, a former senior executive from the CIA and the FBI, a former director of the Defense Intelligence Agency, the head of a national academy on public health, two retired flag-rank military officers, the head of a national law enforcement foundation. But what truly makes this panel special and, therefore, causes its pronouncement to carry significantly more weight, is the contribution from the members of the panel from the rest of the country:

- Three directors and one deputy director of state emergency management agencies, from California, Iowa, Indiana and Virginia, two of whom now also serve their Governor's as Homeland Security Advisors of the Deputy
- A state epidemiologist and director of a state public health agency
- A city manager of a mid-size city
- The chief of police of a suburban city in a major metropolitan area
- Senior professional and volunteer fire fighters
- A senior emergency medical services officer of a major metropolitan area

These are representatives of the true "first responders"—those heroic men and women who put their lives on the line every day for the public health and safety of all Americans. Moreover, so many of these panel members are also national leaders in their professions: our EMS member is a past president of the national association of emergency medical technicians; one of our emergency managers is the past president of her national association; our law officer is president-elect of

the international association; our epidemiologist is past president of her professional organization.

Read our reports and you will understand what that expertise has meant to the policy recommendations that we have made, especially for the events of September 11 last year.

In Memoriam

Those attacks continue to carry much poignancy for us, because they created an empty seat at our panel table. At a few minutes after 10 o'clock that morning, Ray Downey, Department Deputy Chief and chief-in-charge of Special Operations Command, Fire Department of the City of New York—the incident commander at the scene—perished in the collapse of the North tower of the New York World Trade Center. Although the impending disaster had to have been obvious to Ray following the prior collapse of the South tower, he knew and those around him knew their duty. With fearless disregard for their own personal safety, focused entirely on saving the lives of others, Ray and his colleagues all stayed at their post, doing their job. The result of that decision, clear now in retrospect, was the rescue of literally thousands of people from those towers. Ray and 342 of his colleagues paid the supreme sacrifice, and all humanity must acknowledge and be eternally grateful for their actions.

Our loss is tempered by the extraordinary opportunity that we had in being informed and counseled by Ray. Ray Downey served as a dedicated member of the Advisory Panel during its initial three-year tenure, bringing insightful first-responders' perspectives and consistently providing invaluable counsel based on his years of training, unequaled leadership, and exceptional experience in the field.

Ray was not only a nationally recognized leader, author, and lecturer on rescue, collapse operations, and terrorism emergency response. He readily responded to the call for help in Oklahoma City, Atlanta, and other disasters outside his home jurisdiction. Frank Keating is better than I at revealing just how much a hero Ray is to Oklahomans as he is to he own city. Ray was never one to talk about his accomplishments. It has only become more widely publicly known since September that Ray was *the most decorated member* in the entire history of the FDNY—21 times for valor.

Yet, with all of his professional responsibilities, Ray made time to spend with his family, never missing a major school or sporting event of his five children. To the very end, he continued that amazing record with his grandchildren. Two of his sons are now officers of the Fire Department of the City of New York. All five, as well as two of his grandchildren, spoke passionately and eloquently at Ray's memorial service of his total commitment to his family.

It was with great humility but also with great pride that we dedicated our third report to Ray Downey. That report was issued, totally coincidentally—or perhaps providentially—on the same day that Ray's memorial service was held, December 15, 2001. On that day, thousands of firefighters and other first responders from New York and from all over the United States stood in frigid weather for more than three hours—in formation—outside Ray's small parish church on Long Island, while Ray's children and grandchildren, his colleagues, his commissioner, his mayor, his governor, and his president all paid tribute to this remarkable American hero.

Our memorial epitaph to Ray was simple but never more profound:

Ray Downey

Husband . . . Father . . . Patriot . . . Hero . . .

Friend

And in the final, most courageous moments of his duty-filled life . . .

Brother to all Humanity

Ray, we salute you; we know that you are still with us in spirit. With a renewed sense of profound commitment, we pledge on our honor that you and all the other victims of the attacks will not be forgotten and that the loss we have all suffered will not have been in vain.

Our Continuing Mission

Chairmen and Members, our mission remains urgent and clear: we must continue to bolster our capability to thwart terrorists wherever and whoever they are. Our collective call is to continue the momentum to secure our homeland and protect our citizens. While there is much more work to be done, I am confident that we will be successful. America's strength is in its people, our leaders, and our collective commitment, especially during times of crisis.

General Observations on Intelligence and Information Sharing

In the course of our deliberations, the Advisory Panel has been guided by several basic observations and assumptions that have helped to inform our conclusions and policy recommendations for improving our preparedness to combat terrorism.

First, all terrorism is "local," or at least will start locally. That fact has a lot to do, in our view, with the emphasis, the priorities, and the allocation of resources to address requirements. September 11 was further proof of that basic assumption.

Second, a major attack anywhere inside our borders will likely be beyond the response capabilities of a local jurisdiction, and will, therefore, require outside help—

perhaps from other local jurisdictions, from that jurisdiction's state government or multiple state resources, perhaps from the Federal government, if the attack is significant enough to exhaust other resources. That principle was likewise validated last year.

Given those two factors, our approach to combating terrorism should be from the "bottom up"—with the requirements of State and local response entities foremost in mind.

Based on a significant amount of analysis and discussion, we have been of the view that few major structural or legal changes are required to improve our collective efforts; and that the "first order" challenges are policy and better organization—not simply more money or new technology.

Those principles have guided the panel's deliberations on policy recommendations throughout its tenure. And they are nowhere more clear than in matters of intelligence and information sharing.

The chart attached to this testimony is an attempt to depict graphically the magnitude of the problem and the necessary interrelationships that must exist among entities at the local, State, and Federal levels. It shows that integration must exist both vertically and horizontally among various functions and the agencies that have responsibilities for executing those functions. That interrelationship clearly identifies just how important intelligence and information sharing really is to the entire process, across all functions, and at all levels. It also emphasizes our view that simplistic categories such as "crisis management" and "consequence management" do not adequately describe the full spectrum of functions or responsibilities. We are pleased that the new National Strategy for Homeland Security has eliminated the use of those terms.

Moreover, the Panel has further refined its discussion to include the critical need for elements of the private sector to be involved in the sharing of information, especially where their roles have significant national security implications. Those interrelationships are not included in the attached chart.

Our Reports

In our first three reports, the advisory panel has, through its assessments and recommendations, laid a firm foundation for actions that must be taken across a broad spectrum of threats in a number of strategic and functional contexts to address this problem more effectively.

First Report—Assessing the Threat

The Advisory Panel produced a comprehensive assessment in its first report of the terrorist threat inside our borders, with a focus on chemical, biological, radiological, and nuclear (CBRN) weapons. The very thorough analysis in that report can be summarized:

> The Panel concludes that the Nation must be prepared for the entire spectrum of potential terrorist threats – both the unprecedented higher-consequence attack, as well as the historically more frequent, lesser-consequence terrorist attack, which the Panel believes is more likely in the near term. Conventional explosives, traditionally a favorite tool of the terrorist, will likely remain the terrorist weapon of choice in the near term as well. Whether smaller-scale CBRN or conventional, any such lower-consequence event—at least in terms of casualties or destruction—could, nevertheless, accomplish one or more terrorist objectives: exhausting response capabilities, instilling fear, undermining government credibility, or provoking an overreaction by the government. With that in mind, the Panel's report urges a more balanced approach, so that not only higher-consequence scenarios will be considered, but that increasing attention must now also be paid to the historically more frequent, more probable, lesser-consequence attack, especially in terms of policy implications for budget priorities or the allocation of other resources, to optimize local response capabilities. A singular focus on preparing for an event potentially affecting thousands or tens of thousands may result in a smaller, but nevertheless lethal attack involving dozens failing to receive an appropriate response in the first critical minutes and hours.

> While noting that the technology currently exists that would allow terrorists to produce one of several lethal CBRN weapons, the report also describes the current difficulties in acquiring or developing and in maintaining, handling, testing, transporting, and delivering a device that truly has the capability to cause "mass casualties."

We suggest that that analysis is still fully valid today.

Second Report—Toward a National Strategy for Combating Terrorism

By the second year, the Advisory Panel shifted its emphasis to specific policy recommendations for the Executive and the Congress and a broad programmatic assessment and functional recommendations for consideration in developing an effective national strategy.

The capstone recommendation in the second report was the need for a comprehensive, coherent, functional national strategy: ***The President should develop and present to the Congress a national strategy for combating terrorism within one year of assuming office.*** As part of that recommendation, the panel identified the essential characteristics for a national strategy:

- It must be truly *national* in scope, not just Federal.
- It must be comprehensive, encompassing the full spectrum of *deterrence, prevention, preparedness, and response* against domestic and international threats.
- For domestic programs, it must be *responsive to* requirements from and fully *coordinated with state and local officials* as partners throughout the development and implementation process.
- It should be *built on existing emergency response systems.*
- It must *include all key functional domains*—intelligence, law enforcement, fire services, emergency medical services, public health, medical care providers, emergency management, and the military.
- It must be *fully resourced* and based on *measurable performance.*

Of course, the Panel recognizes that in light of September 11, 2001 this objective has been difficult to achieve. However, the principles contained within this strategy and their requirements remain the same.

The Second Annual Report included a discussion of more effective Federal structures to address the national efforts to combat terrorism. We determined that the solutions offered by others who have studied the problem provided only partial answers. The Advisory Panel attempted to craft recommendations to address the full spectrum of issues. Therefore, we submitted the following recommendation: ***The President should establish a senior level coordination entity in the Executive Office of the President.*** The characteristics of the office identified in that recommendation included:

- Director appointed by the President, by and with the advice and consent of the Senate, at "cabinet-level" rank
- Located in the Executive Office of the President
- Authority to exercise certain program and budget controls over those agencies with responsibilities for combating terrorism
- Responsibility for intelligence coordination and analysis
- Tasking for strategy formulation and implementation
- Responsibility for reviewing State and local plans and to serve as an information clearinghouse
- An interdisciplinary Advisory Board to assist in strategy development
- Multidisciplinary staff (including Federal, State, and local expertise)
- No operational control

We included a thorough explanation of each characteristic in our Second Annual Report. For instance, we determined that this office should have the authority to direct the creation, modification, or cessation of programs within the Federal Interagency, and that it have authority to direct modifications to agency budgets and the application of resources. We also recommended that the new entity have authority to review State and geographical area strategic plans and, at the request of State entities, to review local plans or programs for combating terrorism for consistency with the national strategy.

Although not completely structured around our recommendations, the model for the creation of the Office of Homeland Security came from this recommendation.

To complement our recommendations for the federal executive structure, we also included the following recommendation for the Congress: ***The Congress should establish a Special Committee for Combating Terrorism—either a joint committee between the Houses or separate committees in each House—to address authority and funding, and to provide congressional oversight, for Federal programs and authority for combating terrorism.*** The philosophy behind this recommendation is much the same as it is for the creation of the office in the Executive Office of the President. There needs to be a focal point in the Congress for the Administration to present its strategy and supporting plans, programs, and budgets, as well as a legislative "clearinghouse" where relevant measures are considered. We recognize that Congress is still in the process of working towards this objective.

In conjunction with these structural recommendations, the Advisory Panel made a number of recommendations addressing functional requirements for the implementation of an effective strategy for combating terrorism. The recommendation listed below are discussed thoroughly in the Second Annual Report:

Enhance Intelligence/Threat Assessments/Information Sharing

- Improve human intelligence by the rescission of that portion of the 1995 guidelines, promulgated by the Director of Central Intelligence, which prohibits the engagement of certain foreign intelligence informants who may have previously been involved in human rights violations
- Improve Measurement and Signature Intelligence (MASINT) through an expansion in research, development, test, and evaluation (RDT&E) of reliable sensors and rapid readout capability and the subsequent fielding of a new generation of MASINT technology based on enhanced RDT&E efforts

- Review statutory and regulatory authorities in an effort to strengthen investigative and enforcement processes
- Improve forensics capabilities to identify and warn of terrorist use of unconventional weapons
- Expand information sharing and improve threat assessments

Foster Better Planning/Coordination/Operations
- Designate the senior emergency management entity in each State as the *focal point* for that State for coordination with the Federal government for preparedness for terrorism
- Improve collective planning among Federal, State, and local entities
- Enhance coordination of programs and activities
- Improve operational command and control of domestic responses
- The President should always designate a Federal civilian agency other than the Department of Defense (DoD) as the Lead Federal Agency

Enhance Training, Equipping, and Exercising
- Improve training through better coordination with State and local jurisdictions
- Make exercise programs more realistic and responsive

Improve Health and Medical Capabilities
- Establish a national advisory board composed of Federal, State, and local public health officials and representatives of public and private medical care providers as an adjunct to the new office, to ensure that such issues are an important part of the national strategy
- Improve health and medical education and training programs through actions that include licensing and certification requirements
- Establish standards and protocols for treatment facilities, laboratories, and reporting mechanisms
- Clarify authorities and procedures for health and medical response
- Medical entities, such as the Joint Commission on Accreditation of Healthcare Organizations, should conduct periodic assessments of medical facilities and capabilities

Promote Better Research and Development and Create National Standards
- That the new office, in coordination with the Office of Science and Technology Policy, develop a comprehensive plan for RDT&E, as a major component of the national strategy
- That the new office, in coordination with the National Institute for Standards and Technology (NIST) and the National Institute for Occupational Safety and Health (NIOSH) establish a national standards program for combating terrorism, focusing on equipment, training, and laboratory processes

Third Report—For Ray Downey

Our Third Annual Report to the President and the Congress builds on findings and recommendations in our First and Second Annual Reports delivered in 1999 and 2000. It reflects a national strategic perspective that encompasses the needs of all three levels of government and the private sector. It seeks to assist those who are dedicated to making our homeland more secure. Our recommendations fall into five categories:

- ✓ *Empowering State and Local Response* by ensuring the men and women on the front line of the war against terrorism inside our borders have the tools and resources needed to counter the murderous actions of terrorists;
- ✓ *Enhancing Health and Medical Capacities,* both public and private, to help ensure our collective ability to identify attacks quickly and correctly, and to treat the full scope of potential casualties from all forms of terrorist attacks;
- ✓ *Strengthening Immigration and Border Controls* to enhance our ability to restrict the movement into this country, by all modes of transportation, of potential terrorists and their weapons and to limit severely their ability to operate within our borders;
- ✓ *Improving Security Against Cyber Attacks* and enhancing related critical infrastructure protection to guard essential government, financial, energy, and other critical sector operations against attack; and
- ✓ *Clarifying the Roles and Missions for Use of the Military* for providing critical and appropriate emergency response and law enforcement related support to civilian authorities.

Mister Chairmen, I should note that the substance of all of the recommendations contained in the third report were approved by the panel at its regular meeting held on August 27 and 28, 2001—Tuesday the 28th being exactly two weeks prior to the attacks of September 11. Although we thoroughly reviewed those recommendations subsequently, the panel unanimously agreed that all were valid and required no supplementation prior to publication.

The recommendations contained in that report, listed below in summary formed, are discussed in detail in the body of the report, and further supported by material in the

report appendices, especially the information from the nationwide survey of State and local responders covering an array of preparedness and response issues.

State and Local Response Capabilities

- Increase and accelerate the sharing of terrorism-related intelligence and threat assessments
- Design training and equipment programs for all-hazards preparedness
- Redesign Federal training and equipment grant programs to include sustainment components
- Increase funding to States and localities for combating terrorism
- Consolidate Federal grant program information and application procedures
- Design Federal preparedness programs to ensure first responder participation, especially volunteers
- Establish an information clearinghouse on Federal programs, assets, and agencies
- Configure Federal military response assets to support and reinforce existing structures and systems

Health and Medical Capabilities

- Implement the AMA Recommendations on Medical Preparedness for Terrorism
- Implement the JCAHO Revised Emergency Standards
- Fully resource the CDC Biological and Chemical Terrorism Strategic Plan
- Fully resource the CDC Laboratory Response Network for Bioterrorism
- Fully resource the CDC Secure and Rapid Communications Networks
- Develop standard medical response models for Federal, State, and local levels
- Reestablish a pre-hospital Emergency Medical Service Program Office
- Revise current EMT and PNST training and refresher curricula
- Increase Federal resources for exercises for State and local health and medical entities
- Establish a government-owned, contractor-operated national vaccine and therapeutics facility
- Review and recommend changes to plans for vaccine stockpiles and critical supplies
- Develop a comprehensive plan for research on terrorism-related health and medical issues
- Review MMRS and NDMS authorities, structures, and capabilities
- Develop an education plan on the legal and procedural issues for health and medical response to terrorism
- Develop on-going public education programs on terrorism causes and effects

Immigration and Border Control

- Create an intergovernmental border advisory group
- Fully integrate all affected entities into local or regional "port security committees"
- Ensure that all border agencies are partners in intelligence collection, analysis, and dissemination
- Create, provide resources for, and mandate participation in a "Border Security Awareness" database system

- Require shippers to submit cargo manifest information simultaneously with shipments transiting U.S. borders
- Establish "Trusted Shipper" programs
- Expand Coast Guard search authority to include U.S. owned—not just "flagged"—vessels
- Expand and consolidate research, development, and integration of sensor, detection, and warning systems
- Increase resources for the U.S. Coast Guard for homeland security missions
- Negotiate more comprehensive treaties and agreements for combating terrorism with Canada and Mexico

Cyber Security
- Include private and State and local representatives on the interagency critical infrastructure advisory panel
- Create a commission to assess and make recommendations on programs for cyber security
- Establish a government funded, not-for-profit entity for cyber detection, alert, and warning functions
- Convene a "summit" to address Federal statutory changes that would enhance cyber assurance
- Create a special "Cyber Court" patterned after the court established in FISA
- Develop and implement a comprehensive plan for cyber security research, development, test, and evaluation

Use of the Military
- Establish a homeland security under secretary position in the Department of Defense
- Establish a single unified command and control structure to execute all military support to civil authorities
- Develop detailed plans for the use of the military domestically across the spectrum of potential activities
- Expand training and exercises in relevant military units and with Federal, State, and local responders
- Direct new mission areas for the National Guard to provide support to civil authorities
- Publish a compendium of statutory authorities for using the military domestically to combat terrorism
- Improve the military full-time liaison elements in the ten Federal Emergency Management Agency region

Second Report Recommendations on Intelligence and Information Sharing

Mr. Chairmen and Members, please let me expand on the prior recommendations that are directly related to the issues before this joint panel, and let you know what we are also now discussing in this area.

From the inception of our deliberations, we have said that "more can and must be done to provide timely information—up, down, and laterally, at all levels of government—to those who need the information to provide effective deterrence, interdiction, protection, or response to potential threats."[1]

In our Second Report, as noted above, we recommended that an entity be created in the Executive Office of the President similar to, but with much broader responsibilities and authority than, the Office of Homeland Security. As part of that recommendation, we specifically recommended certain responsibilities dealing with Intelligence Coordination and Analysis. We recommended that the office in the White House provide coordination and advocacy for both foreign and domestic terrorism-related intelligence activities, including the development of national net assessments of terrorist threats. We said that a critical task will be to develop, in concert with the Intelligence Community,[2] policies and plans for the dissemination of intelligence and other pertinent information on terrorist threats to designated entities at all levels of government—local, State, and Federal.

We recommended that there be an Assistant Director for Intelligence in that Office to direct the intelligence function for Combating Terrorism, who should be "dual-hatted" as the National Intelligence Officer (NIO) for Combating Terrorism at the National Intelligence Council. We said that the Assistant Director/NIO and staff would be responsible for compiling terrorism intelligence products from the various agencies, for providing national-level threat assessments for inclusion in the national strategy, and for producing composite or "fused" products for dissemination to designated Federal, State, and local entities, as appropriate. The Assistant Director/NIO should be delegated,

---

[1] First Report, p. 57.
[2] Including its Federal law enforcement components.

by Executive Order or in enabling legislation, tasking authority for terrorism-related intelligence collection and analysis. We recommended that that person serve as focal point for developing policy for combating terrorism intelligence matters, keeping the policymaking and operational aspects of intelligence collection and analysis separate. We argued that the Assistant Director would also be the logical interface with the intelligence oversight committees of the Congress. It is, in our view, important to have a senior-level position created for this purpose, and we recommended that the person initially chosen to fill the position be a current or former agent of the Federal Bureau of Investigation, and then be filled in rotation by appropriately qualified persons from law enforcement and the Intelligence Community. Importantly, we said that the intelligence office should be staffed with knowledgeable and experienced personnel, who understand collection, analysis, and assessment processes, from the various intelligence and law enforcement agencies.

To assist in that intelligence function, we recommended the establishment of a "Council to Coordinate Intelligence for Combating Terrorism," to provide strategic direction for intelligence collection and analysis, as well as a clearance mechanism for product dissemination and other related activities. It should consist of the heads of the various Intelligence Community entities and State and local representatives who have been granted appropriate security clearance. We said then, December 2000, that the Director of the Federal Bureau of Investigation and the Director of Central Intelligence should chair it in annual rotation.

Human Intelligence (HUMINT)

Recent events have emphasized the need for the best possible intelligence. Moreover, reliance on sophisticated "National Technical Means" or other high-technology systems is not always sufficient to provide the necessary and timely "indication and warning" to forestall or to defend against a terrorist attack.

In our Second Report (December 2000), we noted that certain procedures, well intentioned when implemented, were hampering the nation's ability to collect the most useful intelligence. For that reason, we recommended the rescission of that portion of the 1995 guidelines, promulgated by the Director of Central Intelligence, which prohibited the engagement of certain foreign intelligence informants who may have previously been involved in human rights violations. Unfortunately, that recommendation was not acted upon before last September 11. It took Congressional action last fall to correct that situation.

Measurement and Signature Intelligence (MASINT)

As the potential grows for terrorists to use more unconventional and sophisticated weapons, especially with chemical or biological agents, our capability to detect such agents assumes greater urgency and requires new technology to provide needed capability.

To meet that challenge, we recommended an expansion and improvement in research, development, test, and evaluation (RDT&E) of reliable sensors and rapid readout capability, and the subsequent fielding of a new generation of MASINT

technology based on enhanced RDT&E efforts. Our goal for sensors and rapid readout technology for chemical and biological agents should be no less than our current capability for nuclear and radiological agents. Much is being done in that area; more is needed.

Statutory and Regulatory Authorities

With a full appreciation for out important and unique civil rights and liberties, we proposed, almost two years ago, important steps to improve intelligence collection, analysis, and dissemination.

We recommended a thorough review, by a panel of Department of Justice (DOJ) officials and knowledgeable citizens outside the Federal government, of the terrorism portion of the Attorney General's "Domestic Guidelines." We examined the guidelines, which establish conditions under which an FBI agent can open an inquiry into possible terrorist activity inside the United States. The guidelines appeared to us to be adequate in scope but have been rendered confusing and ambiguous by successive redrafting over the years, leading to misunderstanding and uneven application among law enforcement agents. We did not suggest that the guidelines be rescinded or that the underlying requirement for them is not sound. We recommended that the panel review the domestic guidelines for clarity, in the interests of strengthening them, while providing for the protection of civil rights and liberties. We also recommended that the guidelines provide examples of permissible and impermissible activity as further information for agents' decisions. Again, it took the events of last Fall to cause that to happen.

The Foreign Intelligence Surveillance Act (FISA) governs domestic national security investigations.[3] The procedures in place in the year 2000 of the Office of Intelligence Policy and Review (OIPR) in the Department of Justice, required to present a matter to the special Foreign Intelligence Surveillance Court established under FISA, required far more justification than the Act does. We recommended at that time that the Attorney General direct OIPR to modify its procedures to conform to the FISA statutory requirements. That did not happen until after the events of last fall, and with additional prodding from the Congress.

Controls inside our borders that can hamper efforts of potential terrorists—be they foreign or domestic—by denying them their "tools of the trade," can be established or strengthened without additional authority. We recommended that the Department of Justice, in consultation with appropriate committees of the Congress as well as knowledgeable members of the scientific, health, and medical communities, and State and local government, continually review existing statutory authorities and regulations. The purpose would be to propose specific prohibitions, or at least mandatory reporting procedures, on the domestic sale and purchase of precursors and special equipment that pose a direct, significant risk of being used to make and deliver CBRN weapons or agents.[4] Some improvements have been made in this area; others are still urgently needed.

[3] 50 U.S. Code, Sections 1801–1863.
[4] An identification of such precursors and equipment should be made in an Executive Order or regulations, coordinated with all relevant Federal health and law enforcement agencies.

Forensics Capabilities to Identify Terrorist Unconventional Weapons

We have today effective forensic capabilities to detect and identify conventional weapons, including high-explosive devices and associated mechanisms, as well as sophisticated techniques for identifying perpetrators.[5]

Given the potential for terrorists to resort to chemical and biological weapons, developing a comparable forensics capability for such weapons is a clear priority. In 2000, we recommended that the federal government foster research and development in forensics technology and analysis. Those steps will involve either the development of a new program in a specific agency, or the consolidation of several existing programs. We also recommended the implementation of an Indications and Warning System for the rapid dissemination of information developed by enhanced forensics. If we can improve significantly our forensics capability, the new national alert system would much more effective in disseminating information on credible threats.

These efforts should include Federal assistance to State and local forensics capabilities. Some terrorist threats or actual attacks may initially appear to be some other form of criminal conduct, and Federal involvement may not be implicated. Enhancements at State and local agencies will not only facilitate early identification, but will also support subsequent criminal investigations.

If terrorists know that the nation has the capability to detect and identify devices and perpetrators—so that the "return address" can be determined—deterrence is enhanced accordingly.

[5] The FBI's internal laboratory and others available to it collectively are, without question, the best in the world.

Information Sharing and Improved Threat Assessments

Several agencies have made strides in enhancing information sharing. Notable examples include efforts by the FBI to implement fully its Joint Terrorism Task Force (JTTF) program and to provide information on combating terrorism to response entities through its web-based system, Law Enforcement Online ("LEO"), as well as the formation of the US Attorneys Anti-Terrorism Task Forces. The Panel has anecdotal evidence to suggest that these efforts, while well intentioned, continuing to be confusing, duplicative, non-standard, and bifurcated in both structure and implementation.

In 2000, we determined that a comprehensive dissemination system must be developed to provide information through expanded law enforcement channels, and through regional FEMA offices into State emergency management channels, for further dissemination to local response entities. As part of that process, we recommended the creation of a system for providing some form of security clearance to selected State and local officials nationwide, and methods for disseminating classified information to those officials in near real time. We said that one product of that process should be timely threat assessments, in which the FBI must be an integral part. The FBI had, in 2000, undergone a reorganization that consolidated several related entities into a new Counterterrorism Division, with an Assistant Director at its head. We said that that division needed more internal analytic capability. As a result, we recommended that the FBI consider implementing a "Reports Officer" or similar system, analogous to the process used by the Central Intelligence Agency, for tracking and analyzing terrorism indicators and warnings. Once again, it took the events of last year for that imperative to sink in.

To promote the broadest dissemination of information to the largest audience of response entities, we recommended, in December 2000, that the Federal government develop a protected, Internet-based, single-source web page system, linking appropriate combating terrorism information and databases across all applicable functional disciplines. The new National Strategy for Homeland Security now calls for exactly that type of system, consistent with our recommendation in the 2nd report.

Third Report Recommendations on Intelligence and Information Sharing

As noted earlier, the Advisory Panel held a regular meeting on August 27 and 28, 2001. Among its approved list of recommendations are those dealing with intelligence and information sharing, described below. At an emergency meeting of the Panel two weeks *after* the attacks, the Panel reconfirmed each of those recommendations approved before the attacks and did not add a single new one.

Sharing Intelligence

For that Third Report, we conducted a nationwide survey of state and local response entities. All State and local organizations surveyed strongly indicated that the Federal government should provide threat and risk assessment information and that the Federal government should provide intelligence about terrorist activities. As a result, we recommended that agencies of the Federal government increase and accelerate the sharing of terrorism-related threat assessments and intelligence with appropriate State and local officials and response organizations. Steps taken by the Attorney General for U.S. Attorneys to develop protocols for sharing more information developed at the Federal level with States and localities, provisions in the USA PATRIOT Act of 2001, and initiatives by the Congress could significantly enhance preparedness and response. In making the announcement of new Justice Department initiatives, the Attorney General

said, "Increased sharing of information among law enforcement and national security personnel at all levels of government are critical to the common effort to prevent and disrupt terrorist acts. To win the war on terrorism, Federal prosecutors and law enforcement personnel must develop and implement effective procedures for information-sharing and cooperation with their State and local counterparts."[6] The challenge continues to be to put protocols effectively into practice. It is critical that procedures for sharing appropriate information with non-law enforcement entities also be developed. State and local agencies response agencies, including public health, must be equal and fully informed partners in the national effort to identify potential incidents and to respond effectively when they occur. For example, when a possible biological threat is identified, sharing information with public health entities, which can inform further communications with public and private medical care providers, will facilitate targeted disease surveillance, resulting in more rapid identification and treatment of potential victims. There continues to be anecdotal information about the difficulty and expense of getting state and local officials cleared to receive classified information.

Better Information

Our survey of state and local responders strongly indicated that they are not aware of what is available from the Federal government, both in terms of programs and offices to promote preparedness and, to a lesser degree, what specialized assets are available to support response to a particular type of incident. This lack of awareness of important Federal preparedness programs may inhibit the preparedness of State and local organizations. It also may delay the summoning of Federal support assets by local and

[6] Memorandum from The Attorney General of the United States to all United States Attorneys, Subject: Cooperation with State and Local Officials in the Fight Against Terrorism, November 13, 2001.

State responders in the event of an incident. Furthermore, in the short term, as the Federal government reorganizes to combat the terrorist threat, confusion about Federal preparedness programs and Federal response assets could increase. As a result, we recommend that the Office of Homeland Security serve as a clearinghouse for information about Federal programs, assets, and agencies with responsibilities for combating terrorism.

The chapter in our December 2001 report on border security also contained recommendations for improving intelligence and information sharing. Having catalogued the complexity of the border problem we set forth explicit proposals for improvement.

Border Intelligence Collection and Analysis

We recommended that the Office of Homeland Security ensure that all agencies with border responsibilities are included as full partners in the intelligence collection, analysis, and dissemination process, as related to border issues.[7]

This process is a "two-way street;" all entities involved must be willing to share information, horizontally and vertically. This will represent a departure from the current "culture" of many agencies to cloister information. We again encouraged the Office of Homeland Security to consider the structure and procedures in our second report for the establishment of intelligence oversight through an advisory board under that office and

[7] The Attorney General, in coordination with other Federal agencies, recently established the "Foreign Terrorist Tracking Task Force." The purpose of the Task Force is to gather, coordinate, and disseminate information (including intelligence and other national security information) among law enforcement and other appropriate agencies (including the State Department) to enable them to have extensive, real-time information on potential terrorists and terrorist activities.

for the establishment of intelligence tasking, collection, analysis, and assessment capabilities in that office.[8]

Information Sharing

The full, timely analysis and dissemination of information among affected Federal, State, and local agencies may be critical in preventing the movement of foreign terrorists and their weapons across our borders. Some interagency agreements for border security do exist, notably the Memorandum of Agreement on Maritime Domain Awareness among the Department of Defense, the U.S. Coast Guard, the U.S. Immigration and Naturalization Service, and the Department of State.[9] We said last year that the Congress needs to revisit the funding for such programs; all affected agencies are not involved in a fully coordinated and integrated process. As acknowledged by several Federal agencies:

> [N]o single framework exists to effectively look at threats across the broad spectrum of issues. What is necessary is the establishment of an organization structure with the connectivity to create a virtual national data repository with the supporting analytical and communications capabilities to develop effective maritime awareness and coordinate appropriate response.[10]

As a result, we recommended that the Office of Homeland Security create a "Border Security Awareness" database system to collect and disseminate information about immigration and border control; and that the Congress mandate participation of relevant Federal agencies and provide adequate resources to fund it. The system could be modeled on the existing U.S. Coast Guard Maritime Domain Awareness program. That

---

[8] *Second Annual Report*, p. 11.
[9] See Appendix R.
[10] Ibid, p. R-2.

program could be expanded to create an interactive and fully integrated database system for all border security matters.[11] It should include participation from all relevant U.S. government agencies, and State and local partners. These issues are now in large measure before the Congress in its consideration of the new Department of Homeland Security.

Our Current Deliberations

Chairman and Members, we continue to believe that improvements in intelligence and information sharing are central to the nation's efforts to combat terrorism. They are, as we see it, the most crucial and fundamental requirement. As a result, we continue to consider—including at a Panel meeting as recently as yesterday—ways to improve both structure and process in this area as we build our Fourth Annual Report to the President and the Congress, due December 15. The creation of the new Department of Homeland Security will not solve all of these issues. In some ways, it may in fact impede the appropriate collection, analysis, and dissemination of intelligence and information. It will, it appears, be yet another "customer" of intelligence for the Intelligence Community, and will have no collection and little analytical capability of its own. Its creation will, for example, also do little to solve the problem of the FBI recasting its efforts from purely law enforcement to detection and prevention.

Conclusion

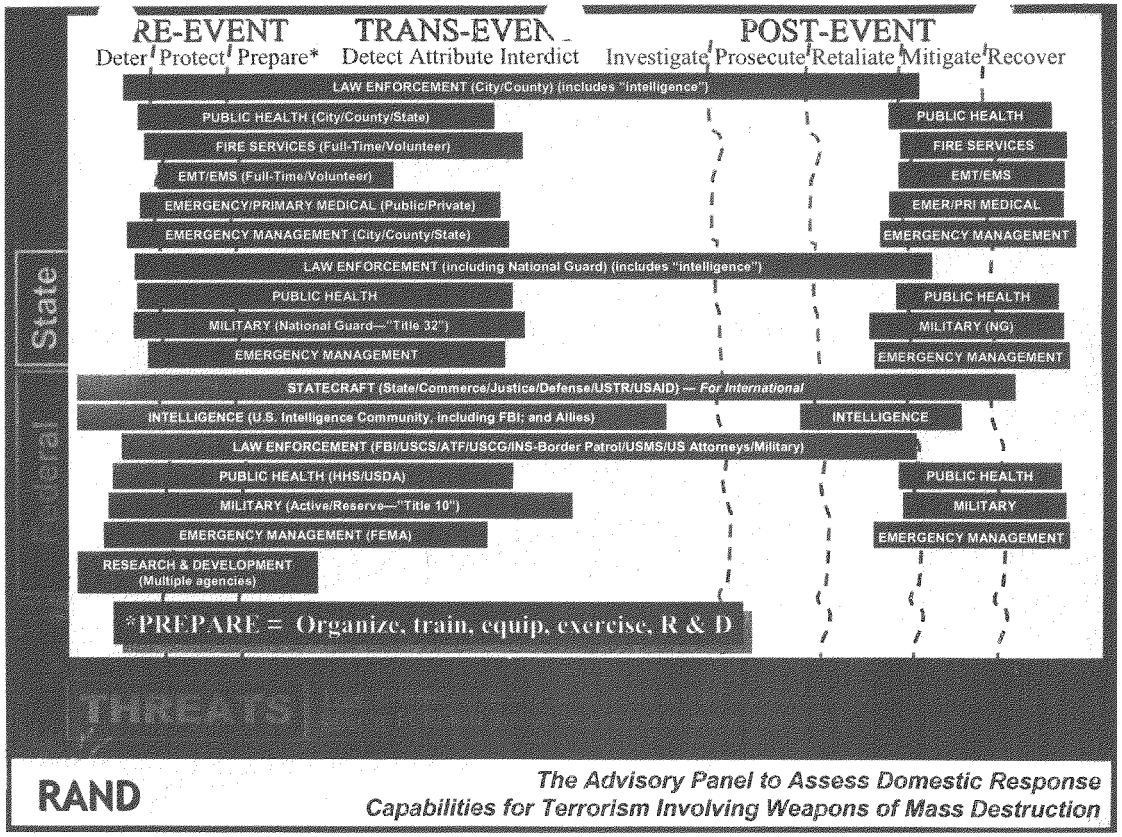
The Advisory Panel will continue to be prudent and judicious in its recommendations, especially those dealing with intelligence and information, always

[11] James Ziglar, Commissioner of the Immigration and Naturalization Service, announced on December 6 that INS will enter the names of more than 300,000 foreign nationals, who have remained in the country illegally after they were ordered deported, into the FBI's National Crime Information Center database. Previously, the government did not pursue most people who ignored orders to leave the country.

considering as an overarching concern the impact of any legal, policy, or process changes on our civil rights and liberties. But we will also be decidedly outspoken on matters that we believe need to be addressed, and will be relentless in our pursuit of the best solutions.

Chairmen and committee members, this is not a partisan political issue. It is one that goes to the very heart of our national security, our public safety, and our uniquely American way of life. We have members on our panel who identify with each of the major national political parties, and represent views across the entire political spectrum. They represent all levels of government and the private sector, and all the key disciplines that are needed to address these issues effectively. We urge Members on both sides of the aisle, in both Houses of the Congress, to work with the Executive Branch to bring some order to this process and to help provide national leadership and direction to address these critical issues. The proposed Department of Homeland Security represents but one part of the issue. We must not let our focus on this one piece preclude our ability to look at the larger strategic picture in making America safer and more secure.

Thank you again for this opportunity.


RE-EVENT
TRANS-EVEN
POST-EVENT
Deter Protect Prepare* Detect Attribute Interdict Investigate Prosecute Retaliate Mitigate Recover
LAW ENFORCEMENT (City/County) (includes "intelligence")
PUBLIC HEALTH (City/County/State)
FIRE SERVICES (Full-Time/Volunteer)
EMT/EMS (Full-Time/Volunteer)
EMERGENCY/PRIMARY MEDICAL (Public/Private)
EMERGENCY MANAGEMENT (City/County/State)
PUBLIC HEALTH
FIRE SERVICES
EMT/EMS
EMER/PRI MEDICAL
EMERGENCY MANAGEMENT
State
LAW ENFORCEMENT (including National Guard) (includes "intelligence")
PUBLIC HEALTH
MILITARY (National Guard—"Title 32")
EMERGENCY MANAGEMENT
PUBLIC HEALTH
MILITARY (NG)
EMERGENCY MANAGEMENT
STATECRAFT (State/Commerce/Justice/Defense/USTR/USAID) — For International
INTELLIGENCE (U.S. Intelligence Community, including FBI; and Allies)
INTELLIGENCE
LAW ENFORCEMENT (FBI/USCS/ATF/USCG/INS-Border Patrol/USMS/US Attorneys/Military)
PUBLIC HEALTH (HHS/USDA)
MILITARY (Active/Reserve—"Title 10")
EMERGENCY MANAGEMENT (FEMA)
RESEARCH & DEVELOPMENT (Multiple agencies)
PUBLIC HEALTH
MILITARY
EMERGENCY MANAGEMENT
*PREPARE = Organize, train, equip, exercise, R & D
THREATS
RAND
The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction

TESTIMONY OF JAMES GILMORE, III, CHAIRMAN, ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION

Mr. GILMORE. Mr. Chairman, Ranking Members, members of this Joint Commission, thank you very much for the opportunity to be here today in my capacity as chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. You have, as you indicated, the written testimony.

Your staff director has given a very able and wonderful summary in which she discussed the work of our panel, which has been existence since the Congress established it by statute back, I believe, in 1998. We began our work beginning in January of 1999. The panel was initiated by Curt Weldon of Pennsylvania, who has a particular concern, particularly about local responders.

But the entire Congress, Members of both Houses, uniformly supported the creation of our panel that began work back in 1999. The mandate was to assess the terrorist threats and potential for attacks targeted against the homeland here of the United States. Concern was expressed by the Congress as to whether the country was willing or able really to respond appropriately if there was an attack, particularly of a weapon of mass destruction.

As your staff director has indicated, we have given three reports, by statute, on time, in December of each year. The first, in 1999, was an assessment of the threat and was one that expressed concern about the potential for an attack of a weapon of mass destruction but indicated, I thought, that it was less likely than a conventional attack, which we thought was very highly likely. That report and all the other reports and staff work has been staffed by the Rand Corporation at the behest of the Congress.

Mike Wormeth is here today. Mike, if you would please indicate your presence to the members. He has been staff director together with others at Rand and have been very able and helpful to all of us.

The second report built upon the baseline threat, but also indicated some very important policy conclusions in the year 2000. One was that there was a need for a comprehensive national strategy, that a national strategy was necessary to begin to prepare for the very high likelihood that some major terrorist attack would occur on the homeland. The recommendation was not for a Federal strategy and remains not for a Federal strategy. The recommendation is for a national strategy, and that means the inclusion of Federal, State, and local elements in the creation of the national strategy.

Second of all, we recommended that there be an improved structure for the ability to coordinate and establish that national strategy. We recommended a national Office of Homeland Security, and of course, that later became the Ridge Office of Homeland Security. We also recommended, by the way, that office be given significant authority, particularly budgets, certification authority in order to enable it to do the coordination work, but also we recommended that it be Senate confirmable and that way we would pull everybody together.

The third report builds on the first two and focuses detailed work in the areas of border security, the use of States and locals particu-

larly, the health community in preparation against an attack on bioterrorism, the use of the military, which has been a fundamental concern of our commission, because obviously of its civil liberties implications, and so it has to be very carefully handled. And then finally, cyber terrorism. That gives you the background.

Mr. Chairman, with respect to the issue you have asked us to come to speak to you on today, as the staff director indicated throughout our three reports we indicated concern about the issue of intelligence and intelligence-gathering. I might mention, Mr. Chairman, that our commission was due by statute for three years and was to go out of business in December of 2001. Following the 9/11 attacks, this Congress extended the commission. We were extended for two years. We remain an advisor to both bodies of this Congress and available, and we will be issuing additional reports in December of this year and, of course, next year as well, for the fifth year of our commission.

With respect to intelligence and sharing of information, our concern has been expressed continuously over the life of this commission. We did a survey particularly of State and local agencies, a very large survey; over 1,000 survey questionnaires were sent—almost complete response, almost a uniform response across the country to our commission and we learned a great deal and it allowed us what I believe to be a good national perspective.

First and foremost, our commission has expressed concern about lacking of mechanisms to effectively analyze and share intelligence information horizontally across the Federal structure, CIA, FBI, NSA, not to mention the non-intelligence organizations your staff director has so eloquently talked about this morning, the ability to share that information across the Federal areas. And that, of course, is an impediment because of culture and because of turf concerns which we have identified.

In other words there has, up to this point, not been an ability to draw this information together from disparate intelligence organizations and to do what so many have said in the last number of months; the ability to connect the dots just hasn't been there because of this difficulty.

But the second point is equally as important and the least discussed. And it is the concern that we have expressed about the inability to share information, not just horizontally, but vertically, up and down the line, Federal, State and local—the inability to share information with governors, the inability to share information with State emergency operations people, State police, localities, police chiefs, fire commissioners, fire chiefs, health care community people, emergency operations organizations.

This is just as important as the horizontal focus that has been so key to the Congress. Our studies have indicated that to the extent that there has been intelligence-sharing, it has been ad hoc. It has been without a real systematic approach. And what would you expect. With the Intelligence Community, it is within the culture, if not within the statute, that you don't share information. If you do, you are even subject to criminal penalties, not to mention the danger of sharing information and the danger to people who provide it, and the capacities of the United States in order to gather it.

These are the fundamentals. But these things must be overcome by an appropriate system of sharing information, clearing people, training, exercising and establishing so that people who need the information can, in fact, get it. There is a lack of an overarching strategic approach on this matter up to this point.

I will close, Mr. Chairman, by saying we also should point out that a lot has gone right, not just gone wrong, but a lot has gone right. September 11 demonstrated that our citizens arose in a very brave way. Our local responders, who almost always will be the first people on the scene, performed heroically in Virginia and New York.

I was Governor of the State at the time of the Pentagon attack. I was well aware of all that. I visited people in the hospitals. I visited our State troopers and awarded them because of their good work. And we have a lot to say about that.

The last point I will make Mr. Chairman is this: We are a free and open society. That is what we are and this is what makes us Americans. Therefore, we will always be at some level of risk. The challenge that we face is sharing information, establishing a national strategy and putting together the systems necessary to make this country safer while simultaneously and at the same time protecting our freedoms and our values that make us Americans. Our commission believes that we can share information, create it and share it with relevant stakeholders without impinging on any of these American values.

Chairman GRAHAM. Thank you very much, Governor.

Ambassador Taylor.

[The prepared statement of Ambassador Taylor follows:]

TESTIMONY TO THE JOINT CONGRESSIONAL INTELLIGENCE COMMITTEE INQUIRY
October 1, 2002
by
Ambassador Francis X. Taylor
Coordinator for Counterterrorism
Department of State

Mr, Chairman, Committee Members:

I would like to begin by thanking you for this opportunity to discuss an issue of vital importance to America's efforts to combat terrorism, and that is the way we share terrorist-related information within the U.S. government. Information is a key weapon in the global war on terrorism. Having timely and accurate intelligence is essential to disrupt terrorist activity and dismantle terrorist infrastructure. Information is also one of America's key defenses to deter threats and prevent terrorist acts before they happen. It is in its unique offensive and defensive capacities that having access to intelligence and analysis proves critical to fighting terrorism.

I am accompanied today by a wide range of experts from our department. We share in your interest to improve those systems which are designed to ensure that all levels of our government receive critical information necessary to defend America's interests at home and abroad. We owe it to the thousands of innocent Americans who lost their lives nearly a year ago to better these systems, and we look forward to continuing to work with you to do this.

I have served as the State Department's Coordinator for Counterterrorism since July 2001. I will never forget the chilling call I received at my desk on September 11: two planes had struck the World Trade Center towers. America and the world would never be the same. A call soon after from Deputy Secretary of State Armitage summoned me to the State Department's Operations Center, beginning a non-stop effort to help coordinate the U.S. government's response to the attacks.

Without the constant flow of up-to-the-minute data and analysis from the intelligence community, we would not have been able to provide the President, Secretary Powell, and other senior leaders the vital information they needed to formulate a coordinated response. I take my hat off to the many unsung heroes within the Intelligence community and our government, who overcame their personal suffering and dedicated themselves to their work, providing the best intelligence and analysis possible given the difficult circumstances. The relationships forged in those harrowing days has not waned between many State Department employees, myself included, and our friends and colleagues in other agencies in the Intelligence community.

The Office of the Coordinator for Counterterrorism serves as the lead for coordinating international counterterrorism policy within the U.S. government and with foreign governments. The Office of the Coordinator is a major intelligence consumer, rather than an intelligence producer, and our

mission depends on the timely and efficient flow of information on terrorism and terrorist threats. One of our objectives therefore is to enhance the sharing of threat and other counterterrorism intelligence between our government and the many other governments around the world that are contributing to the global war on terrorism. We monitor and analyze information, but are not directly involved in the mechanisms and infrastructure through which data is shared within and between agencies. So, I may have to refer to my colleagues here from other bureaus, such as Intelligence and Research and Consular Affairs, on any detailed questions.

INTERNATIONAL EFFORTS

I would like to emphasize that we at the Department of State are working aggressively with our fellow agencies and international partners to detect, deter, and disrupt terrorist activities around the world. And when terrorist attacks occur, we work cooperatively with intelligence and law enforcement agencies to track down and seek the arrest, extradition or prosecution of the perpetrators.

A key aspect of thee activities is intelligence sharing. For example, since the attacks of September 11, the Department has worked hard to step up U.S. government and international efforts to cut off the funds that terrorist organizations such as al-Qa'ida need to survive. This requires substantial sharing of information and intelligence with many countries.

Again, I would reiterate that as an institution our mission depends on effective and timely sharing. Consequently, we are very supportive of efforts to improve the processes involved and it is the Department's policy to support and seek expansion of our intelligence sharing capacity.

SHARING INFORMATION

Taking up the questions you raised in your letter of invitation, I would note that in addition to the daily telephone and in-person contacts with our colleagues in other agencies, there are several processes and procedures in place at the State Department to receive terrorism-related information from the intelligence community and law enforcement organizations.

The State Department and its overseas posts are integrated into both classified and unclassified electronic communications networks used by other federal agencies, and the State Department both receives and transmits information on terrorism directly through these channels. Additionally, the Bureau of Intelligence and Research (INR) receives terrorism-related sensitive classified intelligence reports from other intelligence community components through dedicated communications, including INTELINK, a web-based communications medium. This data-sharing follows the policies and procedures established by the Director of Central Intelligence for the handling of classified intelligence material.

In 1987, the State Department established the TIPOFF program for the purpose of using biographic information drawn from intelligence products for watchlisting purposes. In 1993, we

established the Visas Viper program as a dedicated telegraphic channel for reporting information on known and suspected terrorists directly to the TIPOFF staff. The Viper channel is used both by our posts overseas and by intelligence agency headquarters in Washington, and can accommodate multiple addresses to facilitate information-sharing among users.

In addition to receiving information through the Viper channel, TIPOFF draws from all sources the information it uses to watchlist terrorists. Independently from TIPOFF, the Bureau of Consular Affairs also received basic biographic data directly from the FBI criminal databases – some of which might include information about terrorists – and feeds that information into the Consular Lookout and Support System (CLASS). All consular officers adjudicating visa applications overseas run checks against that system before issuing a visa.

The Bureau of Diplomatic Security receives information from a variety of sources. Domestically, DS receives information from other federal and local law enforcement agencies directly at the headquarters level and through field offices. Overseas, information is acquired from host governments or other USG sources at our Missions abroad. Data arrives via correspondence, reports, reliable sources, and even untested "walk-ins." The process by which the information is received is often diverse. Once received, DS may forward its information for inclusion in TIPOFF or the CLASS system.

INTERAGENCY GROUPS

Since ramping up our counterterrorism activities over the last year, State Department personnel have participated in – and continue to participate in – a number of interagency organizations and task forces. Consular Affairs is represented at the FBI's Foreign Terrorist Tracking Task Force, the Secret Service's Document Security Alliance Group, and the interagency Migrant Smuggling and Trafficking in Persons Coordination Center. The Bureau of Intelligence and Research (INR) represents the Department on the Interagency Intelligence Committee on Terrorism and the Bureau of Diplomatic Security and the Office of the Coordinator for Counterterrorism also participate in selected committee activities. The Bureau of Diplomatic Security is a member of the FBI's 19 regional Joint Terrorism Task Forces, the National Joint Terrorism Task Force, and the Alien Smuggling Task Force.

Individual employees of the Department have also been integrated into a number of intelligence and law enforcement organizations, including INTERPOL, the Director of Central Intelligence's Interagency Intelligence Committee on Terrorism and the DCI's Counterterrorism Center, the FBI's Foreign Terrorist Tracking Task Force, the Data Management Improvement Act Task Force, and the Office of Homeland Security.

Employees from the Bureau of Consular Affairs participate in several groups working to upgrade border security through improved identification and travel documentation. These include the Federal Smart Card Working Group, the GSA Smart Card and Biometrics Group, the Interagency Working Group on Birth Certificate Standardization, and the INS/Entry/Exit Working Group.

Moreover, the State Department's Visa Office participates in frequent meetings and teleconferences with INS, FBI, CIA, the Social Security Administration, and other agencies to share lookout information and visa data.

State also chairs the Data Share Working Group of the Border Agency Partnership, and Visas Viper committees composed of the many agencies represented at our posts abroad work to coordinate the reporting of terrorism information to Washington and its entry into the TIPOFF system. In addition, my office hosts liaison officers from CIA's Counterterrorism Center and FBI's International Terrorist Operations Section.

These partnerships have been very effective in pursuing the United States's counterterrorism goals, and the sharing of information as its relates to these activities generally has been excellent, though there remains room for improvement. State Department personnel participating in these groups and task forces generally enjoy broad access to terrorism-related information. We offer the same access to CIA and FBI personnel in the State Department.

INFORMATION TECHNOLOGY

Terrorism-related information, especially that used for watchlisting terrorists, is shared within and outside the State Department through a variety of electronic media, in hardcopy, and by oral briefings. For example, the Department's TIPOFF watchlist program receives information electronically and feeds it directly into the Consular Lookout and Support System (CLASS), which is checked by consular officers worldwide as a mandatory step in the visa adjudication process. Under the terms of a 1991 MOU approved by the intelligence and law enforcement communities, that information is also entered into the Interagency Border Inspection System (IBIS) for use by U.S. Immigration and Customs officers at ports-of-entry. In August 2002, the entire TIPOFF database, including full biographic records on nearly 95,000 terrorist names, photos, fingerprints, and online source documentation, was made available on CT-LINK to authorized users from five intelligence community and law enforcement agencies. That information is now instantly available to those users for analytical and law enforcement purposes.

The State Department Bureau of Intelligence and Research (INR) manages web pages available to other members of the intelligence community on two web sites – one classified at the SECRET level, and one at the TOP SECRET level. Every day, INR loads intelligence reports known as "INR Assessments" and other finished intelligence publications onto those sites. Most assessments are published on INTELINK within 24 hours of production and approval. All INR products on counterterrorism loaded onto the TOP SECRET site appear on a dedicated page called "September 11 and Aftermath - The War on Terrorism." INR does not maintain a similar page on the SECRET web site because of resource constraints. INR web pages on both systems are indexed by date, country of interest, and product series for user convenience.

The State Department's Bureau of Consular Affairs (CA) is an innovator in the use of information technology to facilitate information sharing and uses advanced information technology to

make visa lookout information, including terrorist lookouts, available to consular officers around the world on a real-time basis. The Consular Lookout and Support Statement (CLASS) uses sophisticated search algorithms to match lookout information to individual visa applicants. CLASS check is mandatory, and the system will not print a visa until the consular officer has checked and resolved "hits" of the applicant's bio-data against the lookout system data. CLASS records doubled after 9/11. Consistent with the requirements of the USA PATRIOT Act, more than 7 million names of persons with FBI criminal and other name-retrievable records were added to CLASS by August 2002, augmenting 5.8 million name records from State, INS, DEA, and intelligence sources.

In addition to the watchlist information contained in CLASS, the State Department greatly expanded the types of non-lookout data shared with INS following 9/11. Much of the bio-data and photos concerning individual visa cases are replicated in CA's Consolidated Consular Database (CCD) and are shared with INS. The CCD contains records of the past five years' nonimmigrant visa issuances and denials, most including photos. CCD is accessible at all consular posts and is updated from around the world every five minutes. Records of all immigrant visa and nonimmigrant visa issuances have been av to INS online since January 2002, and can be accessed at most ports of entry. U.S. passport application and issuance information is captured in our Passport Files Miniaturization (PFM) system. Scanned images of passport applications are also included in a separate database connected to this system.

The Department's Bureau of Consular Affairs is working with other agencies to establish better means to share data, as well as working to establish a connection to the Open Source Information System (OSIS), an unclassified network widely used by a large number of government agencies. In connection with this latter effort, we are cooperating with other law enforcement and intelligence agencies on the best ways to use the planned connection to provide direct access to data from the CCD. In addition, we have begun to scan visa applications in order to make images of these documents electronically retrievable. We are modifying our software to add over two dozen data fields to the NIV processing system so that this data may be more easily shared with the intelligence and law enforcement communities.

The extent to which counterterrorism information is shared by or with us is, generally speaking, predicated on those missions and the methods vary by jurisdiction. Task forces, such as the regional Joint Terrorism Task Forces or ad hoc task forces, may participate. DS, through its Protective Intelligence and its Protective Liaison Divisions, works with state and local law enforcement on a variety of threats against those we protect. DS participates in a variety of local law enforcement forums – each designed to enhance communication and networking. The critical component in achieving success is that both federal and local law enforcement have a user-friendly, real-time method for communicating threats and responses to terrorist-related incidents.

In addition to DS, other parts of the Department are involved in efforts to share information with local and state law enforcement authorities. The INR TIPOFF program currently does not share information directly with state and local law enforcement agencies due to restrictions on disclosure of

sensitive intelligence information to persons not authorized to receive it. However, an agreement was written after 9/11 that permits TIPOFF to periodically export certain declassified biographic data elements from its database under strictly-controlled conditions to the Foreign Terrorist Tracking Task Force.

Under procedures established by the DCI, classified background information may be provided to authorized FTTTF personnel for law enforcement purposes. The Foreign Terrorist Tracking Task Force has the ability to share certain declassified biographic data with authorized state and local law enforcement officers by means of the FBI's Joint Terrorist Task Forces.

The INR TIPOFF initiative is another example of the Department's efforts to responsibly maximize information sharing. Discussions with the FBI are under way which will permit a portion of the TIPOFF database to be placed in the National Crime Information Center's Violent Gangs and Terrorist Organizations file. Local law enforcement has access to that database.

OVERSEAS ACTIVITIES

Overseas, the Department also facilitates information sharing with foreign law enforcement authorities. Regional security officers, the Department's law enforcement officers at overseas Missions, are responsible for initiating and maintaining an open line of communication with host country law enforcement on a variety of security issues, including terrorism. Of course, the security environment and other factors dictate what method and level of information sharing is appropriate. For example, the Antiterrorism Assistance (ATA) Program may help educate foreign counterparts on the benefits and methodology of information sharing.

The information shared is based on a variety of sources, both USG and others. Its substance may have direct impact on the safety of our employees and Americans overseas. As importantly, it may impact our security at home. What remains critical in the process is that the sharing of the information cannot be considered the end use. Rather, it must be quickly and accurately vetted and applied to have any value.

LEGAL QUESTIONS

In general, the Department of State is more a recipient than a producer of information relevant to terrorist suspects. Department of State-generated information is typically derived from diplomatic sources and thus is not subject to the constraints on dissemination of law enforcement or intelligence information. In the past, the Department has not encountered significant legal barriers to sharing its own information related to terrorist suspects with other agencies. The Department of State did, however, encounter legal barriers that precluded receiving information from other agencies. The USA PATRIOT Act made significant improvements in this area.

Executive Order 12958 (concerning classified national security information), the Privacy Act,

and the Immigration and Nationality Act provide the primary legal framework relevant to the Department's sharing terrorism-related information with other agencies. The procedures most relevant to sharing information relating to terrorism concern the handling of classified information, and the restrictions on dissemination of classified information under O. E. 12958. Since the relevant persons at other federal agencies typically have security clearances, these procedures and restrictions have not generally been an impediment to providing terrorism-related information to other U.S. agencies on a need-to-know basis. Restrictions on dissemination of classified information, however, could be an issue with respect to sharing information with state and local law enforcement authorities.

In some cases, restrictions that third parties place on information they provide to the Department will affect our ability to share that information with other agencies. As E. O. 12958 requires, the Department of State cannot disclose information originally classified by another agency without obtaining authorization from that agency. Some highly-sensitive information the Department receives from other U.S. agencies or that the Department generates itself cannot be distributed beyond the original addresses without the prior approval of the office that originated the information or another appropriate office. While the need to obtain approval before distributing such highly-sensitive information does not, as a practical matter, preclude the Department from sharing sensitive information relating to terrorism, it does impose certain procedural hurdles that must be overcome before such sharing can take place.

The Privacy Act generally restricts disclosure of personal information about U.S. citizens and lawful permanent residents. It has not, in our experience, been an obstacle to sharing information related to terrorist suspects, at least for law enforcement purposes. It is possible in theory, however, that it could restrict disclosure in a particular case, where the information concerned a U.S. citizen or lawful permanent resident, and the disclosure was not consistent with the purpose for which the information was kept. Generally speaking, information-sharing should not be a problem in the context of a law enforcement investigation, but in the context of pure information-gathering for intelligence purposes the Privacy Act could present an obstacle to the sharing of such information between U.S. agencies about U.S. citizens and lawful permanent residents.

Visa records and visa record information are considered confidential and protected from disclosure under section 222(f) of the Immigration and Nationality Act (INA). Because the statute permits the Department to share such information with other USG agencies if it will be used for the enforcement of the laws of the United States, section 222(f) does not restrain our ability to share information on terrorism with other USG agencies for law enforcement purposes. Theoretically, there could be a problem if there were no link whatsoever to enforcement of the laws, but in the context of immigration that seems unlikely. In addition, section 222(f) would not prevent the Department from sharing any information relating to terrorism that the Department had received that might underlie a visa decision but be independent of the visa record itself. Further, Congress recently expanded our ability to share information protected by section 2322(f) with foreign governments, and we can always share such information in discretion when a court certifies that the information is needed in the interests of justice.

Similarly, although alien registration and fingerprint records are confidential by law, such information may be made available to federal, state and local law enforcement agencies, upon request, and to persons or agencies designated by the Attorney General.

FLOW OF INFORMATION

Finally, Mr. Chairman, we believe that the free flow of terrorism-related information within the Department of State and between the Department and other agencies is important. While the flow has not always been unfettered, we see no institutional or organization culture impediments to information-sharing that cannot be successfully resolved.

Bureaus have provided a few examples of areas that need further work. Consular Affairs notes that its Fraud Prevention office has responded to an increased demand from the intelligence community since 9/11 for its information, but so far has received little data in return. There seems to be a lack of understanding within the community of what information would be useful to fraud program managers. We are working on this issue.

As noted earlier, the consular lookout system has been significantly enhanced with biodata from FBI NCIC records. Consular affairs continues to work on two related issues – getting a more comprehensive extract of specific records and obtaining access to the FBI's non-name retrievable information that may pertain to an individual visa applicant's eligibility.

Mr. Chairman, this overview ends my formal testimony. I hope this overview has been useful. If you have any questions, my colleagues and I will do our best to answer them. Thank you.

TESTIMONY OF AMBASSADOR FRANCIS TAYLOR, COORDINATOR FOR COUNTERTERRORISM, DEPARTMENT OF STATE

Ambassador TAYLOR. Mr. Chairman and members of the committee, I am proud to be here this morning to represent the State Department to have the opportunity to discuss this very important and vital issue in America's efforts to combat threats to our society from terrorism. Information, intelligence is a key weapon in the global war on terrorism. Having timely and active intelligence is essential to disrupt terrorist activity and to dismantle terrorist infrastructure.

Mr. Chairman, as you mentioned, I have a detailed statement for the record and I would like to briefly summarize my remarks in that statement. I would start by indicating my great respect for the men and women of the intelligence and law enforcement community of our Nation and the tremendous work they're doing on the front lines in this battle against terrorism.

And certainly their efforts should not, in any way, be diminished by our inability so far to perhaps exchange that information more effectively. They are fighting America's wars today and they're fighting very effectively. The Office of the Coordinator for Counterterrorism, the office I'm privileged to lead, has the responsibility for coordinating the international counterterrorism policy with the U.S. Government and foreign governments around the world. We are a major intelligence consumer rather than a producer of intelligence. Our mission depends on timely and efficient flow of information on terrorism and terrorist threats. It also depends on an open relationship with our international partners in exchange of intelligence information that is so vital in helping them to assist us in the global war on terrorism.

I want to emphasize that our Department has committed itself and our Secretary in working aggressively with our fellow agencies and international partners to make sure that that information is exchanged that allows us to detect, deter and disrupt terrorist activities around the world.

Responding specifically to the questions the committee has asked, the State Department and its overseas posts are integrated, both into the classified and unclassified electronic communications networks used by Federal intelligence agencies. The State Department both receives and transmits information on terrorism directly through those channels. Our Bureau of Intelligence and Research receives terrorism-related sensitive classified information through Intelligence Community components. In 1987, the State Department established a TIPOFF program for the purposes of using biographic information drawn from intelligence products for watchlisting purposes.

In 1993, we established the Visas Viper Program as a dedicated telegraphic channel for reporting information on known and suspected terrorists directly off the TIPOFF database. The Viper channel is used both by our post overseas and by intelligence agency headquarters in Washington, and can accommodate multiple addresses to facilitate information-sharing among its users. Our Bureau of Consular Affairs receives basic biographic data directly from the FBI's criminal databases, some of which might include in-

formation about terrorists, and feeds that information into our consular lookout and support system; we call it CLASS.

All consular offices adjudicating visa applications overseas run checks against that system before a visa is issued. Our Bureau of Diplomatic Security receives information from a variety of sources domestically and from Federal and local law enforcement agencies. Overseas information is acquired from host governments or other U.S. Government sources at our missions abroad. Once received, Diplomatic Security forwards this information for inclusion in TIPOFF or in the CLASS system.

With regard to interagency groups, the State Department participates in a wide variety of interagency organizations and task forces. A few examples: The Bureau of Consular Affairs is represented on the FBI's foreign terrorist tracking task force; the Bureau of Intelligence and Research represents the Department on the Interagency Intelligence Committee on Terrorism; the Bureau of Diplomatic Security is a member of 19 of the FBI's regional joint terrorism task forces and a member of the headquarters joint terrorism task force.

The Department is also integrated into a number of intelligence and law enforcement organizations, including Interpol, the DCI's Interagency Intelligence Committee on Terrorism and DCI's Counterterrorism Center and the Office of Homeland Security. My office hosts liaison officers from both the CIA and FBI international terrorism operation section.

As we turn to information technology, terrorism-related information, especially that used for watchlisting terrorists is shared within and without the State Department through a variety of electronic media. For example, the Department's TIPOFF watchlist program of 85,000 names receives information electronically and feeds it directly into the CLASS system, which is checked by consular offices worldwide. Under the terms of a 1991 MOU approved by the intelligence and law enforcement community, that information is also entered into the interagency border inspection system, IBIS, for use by U.S. Immigration and Customs officers at ports of entry.

In August, 2002, the entire TIPOFF database, including full biographic records on nearly 85,000 terrorist names, photographs, fingerprints and on-line source documentation, was made available on CT Link, counterterrorism link, to authorized users from five Intelligence Community and law enforcement agencies. The State Department Bureau of Intelligence and Research manages Web pages available to other members of the Intelligence Community on two Web sites, one classified at the secret level the other at the top secret level.

The State Department's Bureau for Consular Affairs is an innovator in the use of advanced information technology to make the visa lookout information, including terrorist lookout, available to consular offices around the world on a real-time basis. Consistent with the requirements of the USA PATRIOT Act, more than seven million names of persons within the FBI's criminal and other name-retrievable records were added to the CLASS system by August of 2002, augmenting the more than 5.8 million name records

from State, INS, DEA and intelligence sources contained in that system.

With regard to State and local cooperation, the Department of State understands the benefits of integrating State and local enforcement agencies into its counterterrorism activities in accordance with applicable laws and regulations. The Bureau of Diplomatic Security has 21 offices in the United States having liaison responsibility with State and local law enforcement on a variety of law enforcement issues. Currently, discussions are under way with the FBI which will permit a portion of the TIPOFF database to be placed in the national crime information center's violent gangs and terrorist organizations file for access by local law enforcement on a real-time basis.

When we look at legal questions that affect our ability to exchange information, clearly there were before the passage of the USA PATRIOT Act impediments to the sharing of law enforcement data within our TIPOFF and CLASS system. The PATRIOT Act has made significant improvements in the exchange of that information.

Finally, Mr. Chairman, we believe the free flow of information regarding terrorism within the department and between the department and other agencies of our government, both Federal, State and local, is absolutely the most important thing we can do. While the flow of information has not always been unfettered, we see no institutional or organizational cultural impediments to information-sharing that cannot be successfully be resolved.

Mr. Chairman, that concludes my overview of the testimony. At the conclusion, I would be happy to answer your questions.

Chairman GRAHAM. Thank you very much, Mr. Ambassador.

Mr. Manno.

[The prepared statement of Mr. Manno follows:]

Statement of Claudio Manno
Assistant Under Secretary for Intelligence
Transportation Security Administration
before the
Senate Select Committee on Intelligence
and
House Permanent Select Committee on Intelligence

October 1, 2002

Mr. Chairman and Members of the Select Committees, I am pleased to represent the Department of Transportation and participate in your joint inquiry into the performance of the intelligence community concerning the September 11, 2001, terrorist attacks against the United States. My statement addresses questions posed in your letter of invitation.

You asked about the policies and procedures in place at the Department to receive and act on intelligence information from the Intelligence Community and law enforcement organizations concerning terrorism. It is helpful to look at this issue first in terms of how intelligence relating to terrorism flows from producer agencies of the Intelligence Community to the Department of Transportation (DOT), including the Office of the Secretary, the Federal Aviation Administration (FAA) and the Transportation Security Administration (TSA). The second part of the process concerns how (and how much) information from the Intelligence Community is passed to state and local law enforcement agencies, as well as the private sector.

The mechanisms for passing information by the Intelligence Community (IC) to DOT are well established. DOT (including the Office of the Secretary, FAA and TSA) identifies and updates its intelligence needs in detailed "statements of intelligence interest" or "reading requirements," which the IC producer agencies keep on file to determine which products (both raw intelligence and finished products) DOT receives. To help ensure that the Intelligence Community agencies share pertinent intelligence fully with DOT, section 111(a) of the Aviation Security Improvement Act of 1990 (P.L. 101-604) required "the agencies of the intelligence community [to] . . . ensure that intelligence reports concerning international terrorism are made available . . . to . . . the Department of Transportation and the Federal Aviation Administration." The agencies responsible for producing most of the intelligence DOT receives on terrorism are the Central Intelligence Agency (CIA), the Department of State (DOS), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the Defense Intelligence Agency (DIA).

DOT, especially through TSA, is a full and active participant in the national counterterrorism and law enforcement communities by virtue of its relationships with these agencies. A full-time CIA liaison is posted to the Secretary's Office of Intelligence and Security, and that office has established a part-time liaison position at FBI. FAA has also provided a DOT liaison officer to the National Infrastructure Protection Center at FBI. TSA's Transportation Security Intelligence Service (TSIS) maintains full-time

liaison officers at FBI Headquarters, the CIA Counterterrorism Center, and Diplomatic Security's Office of Intelligence and Threat Analysis at DOS. TSIS plans to post liaison officers in the near future at NSA and DIA as well.

The Office of Intelligence and Security (S-60) has historically been responsible for providing intelligence support to the Secretary of Transportation and his staff, and to the DOT Operating Administrations that do not have organic intelligence capabilities such as FAA and Coast Guard have. Unlike TSA, S-60's current focus is on satisfying the intelligence needs of the Department of Transportation's highest level decision-makers. S-60 still coordinates the intelligence and security needs of the Secretary's Operating Administrations (FRA, FTA, MARAD, Office of Pipeline Safety, FMCSA, and FHWA), along with the IC (FBI, CIA, NSA, DIA), and other federal, state, and local agencies, and private industry.

With respect to transportation modes other than aviation, many of the responsibilities now being assumed by TSA had previously been discharged by S-60. At present, S-60 continues to share information with industry, depending on its sensitivity, either via the Transportation Security Information Report (TSIR) or over a secure telephone. The TSIR is an unclassified product meant for wide distribution to security officials within the transportation sector. The content of the TSIR is generally derived from classified intelligence. If the information cannot be declassified, it is transmitted by secure telephone to representatives of the affected industry who hold the proper security clearance. TSIRs prepared by S-60 are routinely coordinated with TSA and others in the law enforcement and intelligence community.

Until the passage of the Aviation and Transportation Security Act (ATSA), DOT distribution of threat information was severely limited because some of the information had to be disseminated without being protected from release into the public domain. Only the FAA had sufficient authority to share "sensitive security information" (SSI) with the private sector. The ATSA broadened the scope of the FAA's SSI authority and will now give DOT and TSA a much better tool to send sensitive threat related intelligence information to all affected transportation modes.

In addition to the previously mentioned liaison officers, S-60 and TSIS analysts routinely deal with their counterparts at the CIA, FBI, DOS, and the Department of Defense (DOD) at conferences, meetings, and working groups such as the Interagency Intelligence Committee on Terrorism and its subcommittees. Two TSIS analysts are assigned to the National JTTF at FBI Headquarters, and liaison initiatives are also underway to assign TSA criminal investigators to FBI Field Office Joint Terrorism Task Forces (JTTFs). TSA is currently identifying which JTTFs around the country would be best suited for TSA participation. A comprehensive TSA Statement of Investigative Interest is being developed, and consultations with the FBI will be undertaken to finalize a Memorandum of Understanding that reflects TSA's operational and information requirements.

The TSIS officers detailed to DOS, CIA, and the FBI meet the same high personal and professional standards as the regular employees of these agencies. Accordingly, they are fully integrated into these agencies and have the same access and restrictions as the agencies' own employees. This access includes the ability to read and review information that is disseminated externally to other agencies, as well as internal, operational, "in-house" e-mails and message traffic that is not shared with outside agencies. As a result, TSIS liaison officers may know more about a terrorist threat or incident than they are allowed to disclose, and TSIS understands that this is the tradeoff for those agencies' granting the liaison officers access to their information. TSIS fully concurs with such restrictions when they are based on the "need- to-know" principle and the requirement to protect intelligence and law enforcement sources and methods.

Where TSIS has had issues with this arrangement is in the definitions used by those agencies of what constitutes need-to-know for TSA. For example, threat information is routinely shared with TSIS, whereas domestically acquired non-threat information (such as terrorist group presence, intentions, and capabilities) needed to evaluate the threat information is provided less often, because it is considered investigative or law enforcement material rather than intelligence.

Unlike CIA, DOD, and DOS, the FBI has not historically considered itself an intelligence production agency due to the statutory restrictions on the dissemination of information it collects in its investigative role.

TSIS has experienced no significant intelligence-sharing problems with DOS or DOD. With respect to the CIA, those few times where TSIS has had problems resulted from unfamiliarity on the part of CIA personnel with FAA's (now TSA's) mission, roles, and responsibilities.

On a daily basis, S-60 and TSIS receive a steady stream of raw reporting and finished intelligence from DOS, CIA, and DOD. This flow includes items that are sent electronically, hard-copy products received via courier, and cables and finished intelligence TSIS can access and retrieve using INTELINK. In addition, e-mail communications with TSIS liaison officers and the staff of other agencies are sent and received using both classified and unclassified systems. From this inflow, TSIS Watch analysts identify, on average, between one and two hundred classified cables, reports, hard-copy products, faxes, and e-mails each day that merit closer review.

TSIS does not receive a similar flow of daily raw reports and finished intelligence from the FBI. It has received from the Bureau finished, summary intelligence on terrorist groups in the U.S. and an assessment of the threat these groups pose to domestic airports and air carriers. In addition, TSIS occasionally receives cable messages regarding potential threats to transportation or a response to a detailed question or request for assessment that TSIS may have requested via one of its liaison officers. Like other federal agencies, TSIS also receives the FBI's classified Terrorist Threat Warning Notices, intelligence bulletins, BOLO (Be On the Lookout) alerts, NLETS messages, the NIPC daily report, and the FBI's annual summary report of terrorism in the United States.

We expect, however, that the flow of raw background reporting from the FBI will increase in the future. The USA Patriot Act of 2001 authorized the sharing of criminal investigative information with other federal agencies in matters of foreign intelligence and counterintelligence, amending previous laws that had prohibited the FBI from sharing Grand Jury and FISA information. The Act also directs the Attorney General to establish procedures for the disclosure of such information. In October 2001, President Bush noted that the Act contained provisions to reduce the existing barriers to the sharing of information. He stated, "The ability of law enforcement and national security personnel to share this type of information is a critical tool for pursuing the war against terrorism on all fronts." As these changes in the law and in the guidelines become institutionalized in FBI policy, we anticipate an increased flow of intelligence.

The process of getting intelligence from DOT into the hands of those who need it for aviation security at the operational level (both state and local law enforcement and the affected private sector) has been accomplished at FAA (now TSA) primarily through the preparation and issuance of either Security Directives (SDs), Emergency Amendments (EAs), or Information Circulars (ICs). Occasionally, a strategic assessment of the terrorist threat is also disseminated to provide a general overview of the threat environment. Law enforcement officers responsible for security at airports have access to the threat information contained in SDs, EAs, and ICs, which is transmitted to them via the "Airport Law Enforcement Agencies Network" (ALEAN). This information is provided as unclassified, "sensitive security information," which in most cases consists of a declassified version of originally classified information. These declassified versions are prepared by the originating agencies with full knowledge of the intended purpose and recipients of the declassified language. Regulated aviation entities (air carriers and airports) receive the SDs, EAs, and ICs directly. In the case of SDs and EAs, the threat information is coupled with mandated security countermeasures that the air carriers or airport authorities must carry out. For example, watch-listed names are provided to airlines in one of two lists (one list is for individuals who should not be transported unless first cleared by law enforcement; another is for individuals who may be transported, but only after undergoing special security measures reserved for so-called "selectees"). The information is available to individual airline check-in agents, in either a manual or automated form, depending on the specific airline.

In addition to communicating threat information concerning aviation security via SDs, EAs, and ICs, TSA's 24-hour intelligence watch alerts industry representatives to events of potential interest that would not necessarily result in the issuance of SDs, EAs, or ICs. Furthermore, the intelligence watch sometimes relays pertinent information that cannot be declassified (regardless of whether it relates directly to the substance of an individual SD, EA, or IC) via secure telephone to properly cleared industry representatives. While TSA ensures that actionable intelligence is declassified and given broadest possible dissemination to those with a need-to-know, there are on occasion items of information that cannot be declassified, but that help industry decision-makers better understand the general threat climate or the context or rationale for mandated security measures. Thus, while there are no legal or policy obstacles to sharing information at the "sensitive

security information" level—indeed, the information is released in that form for the express purpose of sharing it—information that is classified must be protected in accordance with the laws governing the handling of national security information.

Mr. Chairman and Members of the Committee, we at the Department of Transportation recognize the significance of your efforts on behalf of the American people, and we appreciate the opportunity to participate in these proceedings. They will be significant in ensuring the future safety of our Nation. Thank you.

TESTIMONY OF CLAUDIO MANNO, ASSISTANT UNDER SECRETARY FOR INTELLIGENCE, TRANSPORTATION SECURITY ADMINISTRATION

Mr. MANNO. Mr. Chairman, and members of the Select Committee, I am pleased to represent the Department of the Transportation and participate in your joint inquiry into the performance of the Intelligence Community concerning the events of September 11, 2001, the terrorist attacks against the United States.

My full statement addresses the questions posed in your letter of invitation and I would respectfully request that it be entered into the record. I would like to verbally summarize the points made in my presentation.

Chairman GRAHAM. Mr. Manno, your statement as well as the statements that have been submitted by all the members of the panel will be part of the record of our hearing.

Mr. MANNO. Yes, sir. Thank you. I believe it is important to look at the policies and procedures in place at the Department to receive and act on intelligence information from the Intelligence Community and law enforcement organizations concerning terrorism. It is helpful to look at this issue, first in terms of how terrorism intelligence flows from the producer agencies of the Intelligence Community to the Department of Transportation, the Federal Aviation Administration and the Transportation Security Administration. The second part of the process concerns how the information from the Intelligence Community is passed to the private sector as well as State and local law enforcement agencies. The mechanisms for passing information by the Intelligence Community to DOT are well established. DOT identifies and updates its intelligence needs in detailed statements of intelligence interests. The producer agencies use these to determine what products DOT may receive.

To help ensure that the Intelligence Community agencies share pertinent intelligence with the Department, the Aviation Security Improvement Act of 1990 required "the agencies of the Intelligence Community to ensure that intelligence reports concerning international terrorism are made available to the Department of Transportation and the Federal Aviation Administration." The agencies responsible for producing most of the intelligence that we receive are the CIA, the Department of State, FBI, NSA and DIA. In addition, the Department is active in a number of national counterterrorism and law enforcement community efforts by virtue of its relationship with these agencies.

A full-time liaison officer from CIA is posted to the Secretary's Office of Intelligence and Security and that office established a part-time liaison position at FBI. FAA also has provided a liaison officer to the National Infrastructure Protection Center, the NIPC at FBI. TSA's transportation security intelligence service maintains full-time liaison officers at the FBI headquarters in the newly created National Joint Terrorism Task Force, the CIA's Counterterrorism Center, the State Department Office of Intelligence and Threat Analysis. We also plan to post liaison officers in the near future at NSA and DIA as well as the Office of Homeland Security. Liaison initiatives are also under way to assign TSA personnel to FBI joint terrorism task forces throughout the coun-

try. TSA is currently identifying which task forces around the country would be best suited for TSA participation. The TSIS officers detailed to the State Department, CIA and the FBI meet the same high professional standards as the regular employees of these agencies.

Accordingly, they are fully integrated into these agencies and have the same access and restrictions as the agency's own employees based on the need-to-know principle and the requirement to protect intelligence and law enforcement sources and methods. Historically, where the Department has had issues with this arrangement is in the definitions used by these agencies as to what constitutes need to know. For example, specific threat information may be routinely shared, whereas domestically acquired nonthreat information, such as terrorist group presence and capabilities needed to evaluate threat information is provided less often, because it is considered investigative material rather than intelligence.

Unlike CIA, DOD and the State Department, the FBI has not historically considered itself an intelligence production agency due to the statutory restrictions on the dissemination of information it collects in its investigative role. The Department has experienced no significant intelligence-sharing problems with State or DOD. With respect to CIA, those few times where we have had problems, those resulted from unfamiliarity on the part of CIA personnel with our mission roles and responsibilities. On a daily basis, the Department receives a steady stream of raw reporting and finished intelligence from State Department, DOD. This flow includes items that are sent electronically, hard copy products received via courier and cables and finished intelligence that we can access via community databases. From this in-flow, the analysts on our intelligence watch identify on the average of 100 or 200 cables, reports, hard copy products, faxes and e-mails each day that merit a closer review by us.

Up to now, we have now received a similar daily flow of raw reports and finished intelligence from FBI. We have received summary general intelligence on terrorist groups in the U.S. and an assessment on the threat these groups pose to domestic airports' air carriers. In addition, we occasionally receive cables regarding potential threats to transportation or a response to a detailed question or request for assessment that we may have posed through our liaison officers assigned there.

Like other Federal agencies, we also receive the FBI's classified terrorist threat warning notices, other alerts and the FBI's annual summary report of terrorism in the United States. We expect, however, that the flow of raw background reporting from FBI will increase in the future. The USA PATRIOT Act of 2001 authorized the sharing of criminal investigative information with other federal agencies in matters of foreign intelligence and counterintelligence, amending previous laws that prohibited the FBI from sharing grand jury and FISA information.

So we think this will be helpful. The process of getting intelligence from the Department into the hands of those that need it at the operational level, both State and local, law enforcement and the affected parties in the private sector, has been accomplished

primarily through the preparation and issuance of written notifications such as information circulars and security directives.

As appropriate, strategic assessments of the terrorist threat are also disseminated to provide a general overview of the threat environment. Law enforcement officers responsible for security at airports have access to our notices, which are transmitted to them via the airport law enforcement agency's network or ALEAN. This information is provided as sensitive security information, which in most cases consists of a declassified version of originally classified information. These declassified versions are prepared with the assistance and cooperation of the originating agencies.

Regulated entities, such as air carriers and airports, receive the notices directly. In the case of security directives, the threat information is coupled with mandatory security countermeasures that the air carriers and airport authorities must carry out. For example, watchlisted names are provided to airlines via this process. The information is available to individual airline check-in agents in either manual or automated form depending on the specific airline. In addition to communicating threat information concerning aviation security via written notices, TSA's 24-hour intelligence watch alerts industry representatives to events of potential interest that would not necessarily result in the issuance of written notification. The watch sometimes relays pertinent information that cannot be declassified to properly cleared industry representatives.

Mr. Chairman and members of the committee, we at the Department of Transportation recognize the significance of your efforts. On behalf of the American people and we appreciate the opportunity to participate in these proceedings. I would be happy to answer any questions you may have.

Chairman GRAHAM. Thank you very much, Mr. Manno.

[The prepared statement of Mr. Greene follows:]

STATEMENT

OF

JOSEPH R. GREENE

ASSISTANT COMMISSIONER FOR INVESTIGATIONS

U.S. IMMIGRATION AND NATURALIZATION SERVICE

BEFORE THE

UNITED STATES SENATE
SELECT COMMITTEE ON INTELLIGENCE

AND THE

U.S. HOUSE OF REPRESENTATIVES
PERMANENT SELECT COMMITTEE ON INTELLIGENCE

REGARDING

INFORMATION-SHARING AFTER THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001

TUESDAY, OCTOBER 1, 2002
216 HART SENATE OFFICE BUILDING

2:00 P.M.

I thank you for this opportunity to testify before the Joint Committee, and I am eager to assist you in your inquiry into the performance of the U.S. intelligence community in regards to the September 11, 2001, terrorist attacks on the United States. In particular, I want to add to your understanding of the role the Immigration and Naturalization Service (INS) plays in the collection, analysis, and dissemination of terrorist-related information.

Within hours of the attacks on the Pentagon and World Trade Center, Immigration agents across the country worked to support the FBI in pursuing hundreds of leads, as well as responded to requests for assistance from local law enforcement agencies. INS Special Agents in Headquarters National Security Unit and officers from the Intelligence Division collaborated closely with U.S. intelligence. Within a week of the attacks, the INS had over a thousand agents, fully half the total investigative staff, committed to the September 11 investigation and related counterterrorism work. Months later, the INS Forensic Document Lab helped confirm the identify of "shoe bomber" Richard Reid.

The primary jurisdiction over counterterrorism activities rests with other agencies, most notably the FBI domestically and the CIA and State Department overseas. However, as a result of our exclusive authority to enforce U.S. immigration laws, the INS works diligently to ensure that our counterterrorism responsibilities are fulfilled.

The enforcement of immigration laws both requires and generates a considerable amount of information that can be used to identify, detect, and apprehend suspected terrorists and their supporters. For instance, each year INS conducts more than 500 million inspections at our ports-of-entry, receives nearly 8 million benefit applications and the Border Patrol apprehends 1.2 million aliens. Each of these interactions has the potential to generate intelligence. Currently, there are two primary mechanisms in place to facilitate the flow of this critical information to and from INS: computerized "lookout" systems and interagency liaison.

INS and other Federal agencies maintain a number of databases that provide detailed real-time information to U.S. diplomatic officials abroad, officers at ports-of-entry and along the U.S. border and law enforcement officials in the nation's interior. INS is constantly seeking out opportunities to expand the information contained in our databases. As President Bush stressed, when he signed the Enhanced Border Security and Visa Entry Reform Act in May, "We must know who is coming into our country and why they are coming. ...It is knowledge necessary to make our homeland more secure."

Gaining information about those entering the U.S. is a critical intelligence tool. INS has recently deployed a new Student and Exchange Visitor Information System (SEVIS), an Internet-based system that will greatly improve our ability to track and monitor foreign students. By maintaining critical, up-to-date information about foreign students and exchange visitors, and their dependents, SEVIS will enable us to track foreign students in the United States with far greater speed and accuracy. INS began enrolling educational institutions in SEVIS on July 1, 2002, and SEVIS will be mandatory for all institutions admitting foreign students on January 30, 2002.

In October 2001 INS and the Department of State reached an agreement to begin deploying the Department of State's Consolidated Consular Database at U.S. ports-of-entry, which includes

nonimmigrant visa information and a photograph of the alien. Because of that cooperation, an alien's photograph is now available in secondary inspection to help determine if an alien engaged in fraudulent conduct. That deployment was completed in January 2002. In Miami, where the Consolidated Consular Database was first installed, INS inspectors credit the initiative with detecting 108 fraudulent visa holders in the first six months. INS inspectors using the database in New York caught an alien trying to enter the U.S. on a falsified Russian diplomatic passport. In another instance, a 41-year-old man was discovered using the altered visa of a three-year-old Brazilian boy.

The Interagency Border Inspection System (IBIS), the primary automated screening tool used by both INS and the U.S. Customs Service at ports-of-entry, offers another excellent example of how these lookout systems function. IBIS provides access to many databases, including the FBI National Crime Information Center (NCIC) and includes lookouts from all branches of INS, the FBI, the Customs Service, the Department of State, the Drug Enforcement Administration and various other law enforcement agencies. NCIC is the nation's principal automated law enforcement information-sharing tool, with more than 650,000 federal, state and local officers having on-the-street access to the broad range of information it contains. In addition, IBIS is currently being used to screen applicants in the U.S. for all benefits under immigration laws.

IBIS is supplemented by IDENT, an INS computer system that uses fingerprints to identify aliens our agents and inspectors encounter at U.S. borders. We have successfully integrated "wants and warrants" on foreign-born persons from the NCIC and the FBI into IDENT. As a result, over the past year we have apprehended almost 3,000 aliens wanted for murder, sexual assault and other outstanding criminal charges. With the recent deployment of IDENT to INS offices in the interior, we are now better able to identify criminal aliens residing in the United States.

Another initiative was have undertaken is to expand our knowledge through the National Security Entry-Exit Registration System (NSEERS), which INS began to implement at U.S. ports-of-entry on September 11, 2002. Under NSEERS, INS is fingerprinting and photographing nonimmigrant aliens who may potentially pose a national security risk upon their arrival in the United States. In addition, nonimmigrant aliens are required to register periodically with the INS, allowing us to better verify that they are complying with their nonimmigrant status.

Information technical also plays a vital role in enhancing our working relations with state and local law enforcement agencies who are the first responders to a crisis. The primary tool used for integrating these agencies into our work is the INS Law Enforcement Support Center (LESC) located in Williston, Vermont. Currently, 46 states are linked to the LESC, with the four remaining states, as well as Puerto Rico, in the process of being linked.

The LESC gives all law enforcement officers around-the-clock access to INS records, as well as a link to the NCIC. When a police officer arrests an alien, the LESC can provide vital information and, if necessary, put the officer in touch with an INS officer in the field. The LESC routinely uses a number of INS-maintained databases, including a National Automated Immigration Lookout System (NAILS).

INS has a longstanding Memorandum of Understand with the Department of State, under which

suspected terrorists and associates are entered into NAILS. This is being done using a dedicated system known as TIPOFF, which is administered by the Department of State. When an INS officer has a "hit," our Lookout Unit is contacted, which in turn notifies the Department of State and the INS National Security Unit (NSU). The NSU ensures that local INS or FBI Joint Terrorism Task Force agents are notified and appropriate action taken.

This initaitive highlights both a major advantage and a major disadvantage INS has in the fight against terrorism . I will begin with the latter. As INS currently has no automated information system authorized for the use, processing, or maintenance of classified information, information that the intelligence community provides to Department of State officials for inclusion in TIPOFF must be sanitized before it is uploaded into NAILS. As a result, the information uploaded into NAILS contains no more than names, aliases, and biographic information.

In addition, limits imposed by classification also affects the flexibility of the INS to act on cables it receives from the intelligence community because of the absence of a classified infrastructure. Cable traffic received from the intelligence community is funneled into the INS Command Center, a component of the Headquarters Intelligence Division, and then is sorted through daily by intelligence analysts and agents. Some information we receive cannot, because of its classification level, be transmitted to the INS field offices in its classified form. Since such cables are frequently time-sensitive, it is a challenge, given our resources, to translate the cable into timely action.

As INS works to better integrate itself with the overall domestic security mission electronically through the expanded use of information technology, the agency is also acting to improve its effectiveness by strengthening its relationship and formal liaison with other agencies. Face-to-face contact with other agencies, especially when it occurs routinely, can best foster cooperation and coordination in ways that can never be duplicated by employing computer systems and other information technology, no matter how sophisticated it may be.

INS actively participates in a variety of task forces that were established to deal exclusively with terrorism-related issues. our most extensive direct interaction with other members of the intelligence community occurs through our participation in Joint Terrorism Task Forces (JTTF). INS has been a long-time participant in these FBI-led, multi-agency task forces, which are in place in key metropolitan areas nationwide. JTTF agents are a critical component in our national efforts to root out terrorists and their supporters, and they have done much to increase the level of domestic security. INS Special Agents assigned to JTTFs have conducted more than 6,500 joint interviews since September 11, 2001. In general, we have found our participation, which is coordinated through our National Security Unit (NSU), to be extremely beneficial.

INS also participates in the Attorney General-directed Anti-Terrorist Task Force (ATTF), recently created within U.S. Attorney's offices. In one sense, the ATTFs are similar to the Law Enforcement Coordinating Committees set up years ago under the auspices of the U.S. Attorney. They are a consultative mechanism used to bring together top field officers from various law enforcement agencies to discuss pertinent counterterrorism issues. In another sense, they are quite different in that they can function in a very specific operational manner on selected initiatives, such as the Attorney General's

Voluntary Interview program.

On October 29, 2001, as a result of the issuance of a Presidential Executive Order, the Department of Justice created the Foreign Terrorist Tracking Task Force (FTTTF). The INS has provided key personnel to help ensure the mission fo the FTTTF: to coordinate federal agencies' efforts to identify potential terrorists attempting to enter or remain in the United States.

In addition to these three initiatives, INS has four full-time special agents from our NSU assigned to the National Security Division at FBI headquarters and two assigned to the CIA's Counterterrorist Center. The INS is equipped to immediately supplement NSU resources when events warrant. For example, immediately following September 11, the INS dedicated additional investigators and INS attorneys to the NSU.

Perhaps the greatest impediment to enhancing integration and information-sharing within the intelligence community is resource limitations. As the number of Joint Terrorism Task Force locations have expanded to all federal Judicial Districts, INS has found it difficult to keep pace. We have roughly 2,000 special agents worldwide. In addition to their counterterrorism work, these agents are also responsible for combating alien smuggling, investigating immigration fraud, identifying employers who have violated immigration laws, and other activities that are an essential part of INS' mission.

With our resourees at maximum capacity, it is not surprising that among the challenges facing INS is to thoroughly analyze the information it collects or receives from other agencies. In terms of our anti-terrorism efforts, this may be our greatest challenge. The utility of intelligence information is only as good as our capacity to properly analyze it. Currently, the INS has a cadre of only 200 intelligence officers and analysts worldwide. This small cadre of employees provides a great service to the INS and the other intelligence community and law enforcement agencies. The critical nature of this analytical capability is amplified in light of our limited resources, which we must strategically apply to those who pose the greatest potential threat.

While we recognize all the efforts to improve intelligence analysis and sharing, we also understand that more still needs to be done. INS is deeply committed to that effort. We look forward to working with you to continue providing the American people with the level of security that they demand and deserve.

TESTIMONY OF JOSEPH GREENE, ASSISTANT COMMISSIONER FOR INVESTIGATIONS, U.S. IMMIGRATION AND NATURALIZATION SERVICE

Mr. GREENE. I would like to thank you for the opportunity to testify today on behalf of the INS concerning information and intelligence-sharing within the Federal Government and between Federal, State and local agencies.

INS sees its function in the war against terrorism in two distinct areas: An external role of safeguarding the borders of the United States against the entry of terrorists and their supporters, and an internal role of identifying, locating, apprehending and deporting aliens who pose a threat to the domestic security of the United States or aliens who offer support and assistance to those who might pose such a threat.

I can report to the Joint Committee that since the terrorist attacks on the United States, intelligence-sharing and its application in our work has increased dramatically. Nevertheless, we also recognize that the process of improving intelligence-sharing and joint cooperation in its use is continuous and demands constant commitment on the part of all of the agencies involved.

Regarding our work in safeguarding borders, new cooperation between the INS and the Department of State now permits immigration inspectors to access visa application data during the primary inspection process. These data give inspectors new tools in testing the statements made by an applicant for admission against statements made to consular officers when applying for the visa. In addition, over the past year the use of the Interagency Border Inspection System, IBIS, has been improved with new lookout information, as Ambassador Taylor has indicated, and the INS has expanded the use of that system to include not only applicants for admission into the United States, but also applicants for benefits under the relevant immigration laws.

The most significant changes in information-sharing since the attacks have occurred, however, are in our internal or domestic role. Last month INS began the phased implementation of the National Security Entry-Exit Registration System, NSEERS.

Initially under this system, INS is requiring the fingerprinting and photographing on arrival of individuals who might pose a potential national security risk to the United States. In addition, these people are required to register periodically with the INS, allowing us to better verify that they are complying with the conditions of their non-immigrant status.

INS has begun to deploy the Student and Exchange Visitor Information System, SEVIS, an international-based system that will greatly improve our ability to track and monitor foreign students. This system will greatly enhance our ability to detect those who seek to abuse or exploit our educational and training institutions for unlawful or injurious purposes.

INS special agents have participated in the joint terrorism task forces around the country since 1996. Since the attacks, INS and FBI agents have conducted almost 6,500 joint interviews in connection with the investigation of the attacks themselves or with related counterterrorism investigations. These interviews have resulted in the arrest of over 526 immigration violators solely on the

grounds of immigration law violations in addition to other arrests in connection with the investigation itself.

Finally, a word about INS cooperation and information-sharing with State and local law enforcement agencies. The principal vehicle of the INS for information-sharing with local law enforcement has been the Law Enforcement Support Center, as Ms. Hill indicated. The Law Enforcement Support Center provides real-time information from INS databases to police officers across the country. In 46 States, the process of clearing INS databases is an automated function of the record checks local law enforcement officers routinely conduct. The LESC is staffed 24 hours day, 7 days a week, and provides local police officers with the ability to talk directly to an INS law enforcement technician or special agent about the facts surrounding a specific person in custody.

Furthermore, in August INS entered into a written agreement with the State of Florida under which 35 local law enforcement agencies assigned to regional domestic security task forces in that State were trained in immigration law enforcement and certified to enforce immigration law in connection with their domestic security duties. We are currently engaged in discussions with several other States and localities exploring the possibilities of similar arrangements. These designs significantly increase the level of effective cooperation between the INS and State and local law enforcement officials.

While we recognize that significant progress has been made in intelligence-sharing and in improving the connectivity between the different agencies charged with domestic security law enforcement, we also recognize that still more needs to be done. INS is firmly committed to that effort. We look forward to working with you and the Congress as a whole to increase our domestic security and safety to the level demanded and deserved by our people.

Thank you, Mr. Chairman. I would be happy to take your questions at the end of the statements.

Chairman GRAHAM. Thank you very much, Mr. Greene.

Mr. Andre.

TESTIMONY OF LOUIS ANDRE, SPECIAL ASSISTANT FOR INTELLIGENCE, J–2, DEFENSE INTELLIGENCE AGENCY

Mr. ANDRE. Mr. Chairman, members of the committees, I welcome the opportunity to participate in today's hearings. Thank you very much for the invitation.

The topic of information-sharing is one of exceptional importance and one upon which DIA has focused considerable and specific attention over the past year and a half. Within this topic lies several of the keys to revamping and improving our performance in the war on terrorism.

Within a month of the terrorist attack on the USS *Cole* in October 2000, DIA took a number of steps to enhance its ability to provide timely, actionable terrorism threat intelligence to Department of Defense entities worldwide. The result of those steps is embodied in the Joint Intelligence Task Force for Combatting Terrorism. This reorganization, and, more importantly, process reengineering, was based on two fundamental and deeply held beliefs. Both have to do with today's topic of information-sharing.

The first of these beliefs is that the all-source analysis component of the Intelligence Community, if provided access to a broader base of information, can make a greater contribution to the counterterrorism mission.

The second belief is that there are, indeed, significant amounts of information relevant to the terrorist threat that remain undertapped, underutilized, and/or not subjected to sufficient analytic scrutiny. We believed those two things in the immediate aftermath of the USS *Cole* attack and we believe them today.

There are a variety of reasons why large volumes of information remain under-exploited. Among the most common are strict compartmentalization due to source sensitivity, narrow interpretation of laws or executive orders, misunderstanding or incomplete understanding of one another's missions and requirements, or a too narrow view of what does and does not constitute terrorism-related information.

I would like to expand a little on this last point, the too-narrow view of terrorism information. I think it has particular relevance to today's proceedings.

I believe we have to redefine and significantly broaden the term "HUMINT intelligence collection" when it comes to terrorism intelligence. For example, looking within the Department of Defense, our military security and investigative components, our military police, special agents, gate guards and the like, are not intelligence collectors. But they do gather and not always disseminate considerable amounts of information they deem to be of little or no interest beyond localized security or criminal concerns.

However, this type of information—stolen credentials and identification, attempts to breach security, robberies, license plate thefts, bribery, or even corruption—when put in the larger context by insightful analysts equipped with good tools, holds promise of additional terrorism analysis successes.

Terrorist activity is by its very nature criminal activity and in our search for relevant information, the signal event or the dot that needs to be connected, we must cast a much wider net and then more rigorously mine, examine and interpret the take.

There are no insurmountable legal, security or technical obstacles to significantly expanding the base of information available to our terrorism analysts. Progress is being made. As noted, DIA has made considerable investments designed to optimize its ability to receive, store and fully exploit a wide range of new information.

In my opinion, one of the most prolonged and troubling trends in the Intelligence Community is the degree to which analysts, while being expected to incorporate all sources of information into their assessments, have been systematically separated from the raw material of their trade. How did this happen? The combination of large analytic workforce drawdowns in the early nineties and voluminous streams of collected data led to a need for more "front end" filtering, packaging and producing of raw data. Thus, the interpretive function, determining relevance, importance and meaning of the raw data, moved further inside the organizations that collected the data in the first place.

This is not necessarily a bad thing and I have great respect for those in the processing and exploitation arena who labor to sepa-

rate the nuggets from the noise, to rationalize the irrational and to add value. Theirs is an indispensable function. However, when our so-called all-source analysts are put in the position of basing important judgments on some sources of information or already-interpreted sources of information, that is a bad thing. In the area of terrorism analysis, it can be a tragic thing.

At least for a few highly complex high stakes issues, such as terrorism, where information by its nature is fragmentary, ambiguous and episodic, we need to finds ways to emphatically put the "all" back in the discipline of all-source analysis.

While this is an exceptionally simple concept, I am under no illusions that implementing it will be easy or painless. We will need your help and support to pull that off. I thank you in advance for that support.

Chairman GRAHAM. Thank you, Mr. Andre.

Commissioner Norris.

Senator MIKULSKI. May I exercise a point of personal privilege?

Chairman GRAHAM. Of course.

Senator MIKULSKI. Thank you very much. I am so delighted that the committee asked Commissioner Norris to come and testify today. This is one of really three testimonies he has given on the topic of homeland security. He brings a very incredible background as both a police officer and in a command and leadership position, serving also in New York and most recently significant experiences we have had in Baltimore, and we are part of the capital region. I believe his testimony will be very complimentary to Governor Gilmore's in terms of our first responders and the people on the frontline. I am just delighted that the committee has chosen one of the best of the best to present testimony.

Chairman GRAHAM. Thank you. Commissioner, it doesn't get any better than that.

[The prepared statement of Commissioner Norris follows:]

Senate Select Committee on Intelligence
Tuesday, October 1, 2002
10:00 a.m.
Senate Hart Office Building

Remarks from Baltimore Police Commissioner Edward T. Norris

Good Morning ladies and gentlemen, I'm honored that you have invited me here to speak with you today. I'm proud to represent the Baltimore Police Department, and I hope the information discussed today leads to better intelligence sharing between local and federal agencies. Unfortunately in the past year it has not improved to an acceptable level.

In October of 2001 Baltimore Mayor Martin O'Malley and I testified before the House Committee on Government Reform on this very issue of information sharing. We pointed out that the FBI had less than 12,000 agents at the time, while local law enforcement had nearly 650,000 officers. We stressed that police officers, not federal agents, were in touch with millions of people everyday and we needed to know what the FBI knows about threats, tips, or even just rumors about terrorism. One year later the situation is much the same.

Today I am prepared to share with you several examples of suspicious activity that has taken place in Baltimore. In most of these cases my officers uncovered the information which led to these investigations, and in almost every one of these cases a federal agency did little if anything to work with the Baltimore Police Department. In one particular case a member of the Federal Bureau of Investigation told me they were not investigating a particular suspect. However, after my detectives continued to

research this person, the FBI contacted us to ask why a computer had alerted them that our agency was still looking into this suspect? Despite what I had been told, there was an ongoing investigation on this person.

One of the questions I was asked to discuss today is 'what are the impediments to intelligence sharing among local, state, and federal agencies'? The answer is simple; the federal government is that impediment. Information from federal agencies is still fragmented and inconsistent. When the federal alert status was raised on September 11, 2002 I heard of it the same way the rest of the country did, on television. In the past year I have asked the FBI several times for a full briefing on all Baltimore based investigations involving international/national terrorism; that meeting has never happened. Why have you heard so little about this huge information gap between local and federal law enforcement? Unfortunately, some of the blame must fall on police chiefs throughout the country who privately complain that they have no idea what the feds may be working on in their area...but for reasons known only to them they have decided not to speak out.

In closing, I want to remind you that this new war on terrorism will be most effectively fought through the oldest law enforcement strategy there is, human intelligence. In the end, people deliver bombs, bio-warfare, and bullets...and they are sharing their plans with others. Shouldn't we be doing the same?

The Baltimore office of the FBI has close to 60 agents to cover this city. The INS has 20 special agents assigned here in Baltimore. I have 3200 sworn officers, and more than 500 civilians policing this city. Both the math, and the logic, is staggering.

TESTIMONY OF EDWARD NORRIS, COMMISSIONER OF POLICE, CITY OF BALTIMORE

Mr. NORRIS. It sure doesn't. Is this televised?

Mr. CHAIRMAN, thank you for inviting me. This is my third time testifying. Actually, following the Senator's remarks, I would like to decline to read my written testimony that has been submitted for the record, obviously, but would prefer to share a couple of stories that are going on right now in Baltimore, which as you know is a mid-sized American city, and I would just like to talk about some of the problems we are encountering at the ground level.

I think I have chosen to do this, because after hearing all of the testimony from Governor Gilmore on, I think it kind of underscores the problems we are facing at the very local level, because if indeed the Federal Government says there is a 100 percent chance we will be hit again, and as we have heard from the previous testimony, it is going to be a local response, of course, we are still encountering difficulties defending our cities, despite the improvements made. I would just like to talk about a few of them people may or may not know about. All of them I will talk about I can now, because they have been out in the public or press. I will leave out names and addresses if they are pending investigations.

One of the things I found rather chilling is something that happened on September 10, and I have to go back to my experience with the New York City police about 12 years ago, because there are striking similarities in both the findings and the response.

But on November 5, 1990, I was a lieutenant with the New York City Police Department, and, as we all know, there was an assassination of a radical Jewish leader in the Marriott Hotel on Lexington Avenue in Manhattan. After he was killed, the assassin ran out of the ballroom onto Lexington Avenue, jumped into a Yellow Taxicab, jumped immediately out, was confused, encountered a police officer who he shot, was shot in return fire and wounded at the scene. We had our arrest of our murderer.

Going through his pockets and his papers, obviously we found out where he lived. Upon arriving at his house, we found other gentlemen, also I believe from Egypt, who answered the door. What do you think they did for a living? They were New York City cabdrivers, who admit being at the scene at the time of the homicide. So it was pretty clear to us he jumped in the wrong taxi.

We did a search warrant of the house, and in the warrant we came up with huge, voluminous, according to sources I have spoken to, the biggest al Qa'ida seizure on American soil still. There were photographs of New York City landmarks, writings in Arabic and Farsi, diagrams and notebooks and the like. All these things were seized by us and the New York City police and brought back to my office.

The next day, of course, we gave a briefing to our superiors. The question that was posed to me and my detectives was, can you tell me this man acted alone, a lone gunman, to which the response was of course not. He at least had two other people with him, the getaway drivers.

We were told you shut up. You handle the murder, we will handle the conspiracy, they being the Joint Conspiracy Task Force. From that day on our times were turned over, the cases went in

different directions. We handled the murder, they handled terrorism investigation.

Almost two years later there was an explosion at the World Trade Center. I was summoned back to listen to tapes, review documents and the like, only to find out that those documents that we turned over were not translated until midway through the bombing trial of the first Trade Center attack. The people that I released from my office, one of them actually drove the van into the world Trade Center in '93. This has bothered me for a long time, but is now subject to the book so we can talk about this publicly.

I bring this up because on September 10 of this year in our city, in Baltimore, my detectives were out on a routine arson warrant. They find the subject who they are going to arrest for an arson and harassment, and in the apartment they encounter eight men from various countries, from Morocco, Pakistan, Somalia and Afghanistan. The apartment is very sparsely furnished. There are computers and documents, passports and the like that do not belong to them of people of different names and photographs. There are also photographs of some landmarks like Union Station in Washington, D.C., Times Square, New York.

There are also computers that we seized and cell phones. We got a search warrant for these. They were downloaded by our police department. And in there we find that in the week preceding September 10, which we have to keep in mind is the day we are told we are at a very high state of alert, we find they were on the Internet for hours at a time in the middle of the night checking out web sites such as Learntofly.com, Beapilot.com, all local airports and the like. Further analysis of their hard drive that was erased shows photographs of jetliners and many other things.

The reason we bring this up now is I don't know what these men have or have not done, other than what I have told you. The investigation continues. But several were released by the Federal Government that day. And until—and not only that, worse than that, we were told that there is nothing more than expired visa violations on these folks and there is nothing to indicate the existence of a terrorist cell.

Well, that may be true on its face. I mean, if we are waiting for a notarized plan with a list of terrorists, it is going to be a long wait. This is chillingly, eerily similar to what we encountered years ago and encounter here and there through our daily work as police officers in this country, and to be told this by our Federal partners is very disturbing to us.

And that is where we stand right now. That investigation continues. There are a couple of more anecdotal ones I would like to share with you just as part of what has happened in the year since September 11 to date.

We had two men on September 11 of 2001, the day this country was attacked, who were seen celebrating the World Trade Center attacks by a delivery man who was smart enough to call the police. We went in, talked to them, brought them in for questioning. They were subsequently released, I believe by the FBI; there was no evidence to hold them at the time, which may have been the case.

In June of this year, we were notified and asked for our help very quickly to please apprehend someone. We ran through our in-

telligence division database and, of course, it was on the people from that night. The point of that little story is the fact we had no idea there was a pending investigation on these folks who live in my city.

We also had, as you probably know by now, June 24, Ramzi el-Shanouk was arrested on Lehigh Street in Baltimore. He was a previous roommate with Hani Hanjour, and Nawaf al-Hazmi, the September 11 hijackers. We were notified of this investigation three days before it was taken down. This is the one that I really would like to bring to everyone's attention.

We have a very competent intelligence division in our department, as most major city police departments do. We run our own investigations and we run them pretty well. But we also check with our Federal counterparts to make sure we are not wasting resources and disrupting anybody else's work.

We have someone now we are investigating, he is rather radical in our city. We asked our counterparts, do you have anything going on this? And, of course, we were told absolutely not. We continued with the investigation, and there is a blind hit in one database that alerted them to the fact we are still investigating this subject, at which time we were notified and said can we come talk to you about the person? They said we are not investigating, well, actually we are investigating, and we need to come talk to you about it, but we couldn't really tell you at the time.

There are others. That is enough for now.

The statement I would like to make, the fact is I am representing myself. I don't represent the major city chiefs of the IACP. But there are several local chiefs in this country who feel the same way. Unfortunately, most of them complain privately. When they are public, they don't want to say anything, for what reason is only known to them.

But if we are talking about this as a local response and there is a need to know, who do we think needs to know more than the chiefs, who protect the cities' citizens? We need to know more than anybody in this country what is going on in our cities, yet we don't. I defy anybody, you can call anybody today from any major American city to ask them what is going on in their cities regarding terrorism investigations today. I think you would be surprised at the response.

I think I am going to stop there and answer any questions you may have for me, Senator.

Chairman GRAHAM. Thank you very much, Mr. Commissioner, for a very illuminating set of comments.

We have followed a pattern with these hearings of designating four of our members to be the lead questioners, two from the House, two from the Senate. Each of the questioners will have 20 minutes. The designated lead questioners for today are Senator Wyden, Representative Hoekstra, Senator Shelby, and Representative Bishop.

Representative Bishop has indicated to me that he is about to manage a bill on the House floor, and with the consent of Senator Wyden, he will be called upon first so that he can complete his questioning and meet his other responsibilities.

Senator FEINSTEIN. Mr. Chairman, if I may, after the four lead questioners, would it be your intention to recess for lunch?

Chairman GRAHAM. If the four lead questioners all take their full time, that would put us at approximately 1:00 or close thereto, so, yes, it would be my expectation that we do the lead questioners, break for lunch, reconvene at 2:30.

Senator MIKULSKI. Mr. Chairman, there is a vote at 12:15.

Chairman GRAHAM. The Senators will have to leave to accommodate that.

Congressman Bishop.

Mr. BISHOP. Thank you very much, Mr. Chairman. Let me thank all of our panelists for bringing very, very illuminating testimony to us this morning. Let me begin by saying the joint inquiry has established a number of things, including that the CIA and NSA possessed critically important information on two of the hijackers, Mihdhar and Hazmi, that was buried within the CIA's raw operations cables and the NSA's raw intercepts. Almost no one outside of these agencies was allowed to access these databases of raw HUMINT signals intelligence. CIA and NSA, the analysts, either did not see this information or concluded that it did not reach internal thresholds for reporting or did not appreciate the needs of other agencies for that information. Thus, critical information lay dormant for, in the most basic intelligence databases, over a period approaching two years.

I mentioned a moment ago that counterterrorism analysts outside CIA and NSA cannot access the databases. That is still true today. DOD, FBI, FAA, INS, State Department, none of the analysts at these agencies get to examine the information in these databases.

I am sure it will come as a shock to the public and even members of this joint inquiry that even the proposed Department of Homeland Security under the House version of the bill at least would not be guaranteed access to these databases.

Post-September 11 reviews have revealed over 1,000 CIA reports or cables that contained the names of hundreds of suspected terrorists that were not turned over to watch list agencies. Mihdhar and Hazmi were in all sorts of public and State and Federal databases prior to September 11 through which they could have been found had anyone thought to look.

The Department of Transportation never saw the Phoenix memo, and in hindsight asserts that the memo would have triggered action in DOT had it been passed to them. FBI agents handling the Moussaoui case and the Phoenix memo apparently knew nothing of the history of the Bojinko plot or the attempt by Algerian terrorists to slam a hijacked airliner into the Eiffel Tower in France.

I could go on and on in this vein, but there is a point that is clear. As Ms. Hill testified recently, first, while we cannot conclude that the plot could have been detected if more information had been shared, it is at least a possibility. Second, we obviously could have done much better at information-sharing and must do better in the future if we hope to succeed in foiling future attacks.

Our current mechanisms for information-sharing are human liaison and the exchange of written reports that reflect a filtering of

and the application of judgment to raw intelligence. September 11 proves that these mechanisms alone are inadequate.

As the prepared statements of several of our witnesses today make compellingly clear, broader access to raw intelligence is mandatory, and we must at the same time apply proven computer technology to sift through this massive and detailed data to find correlations, linkages and patterns that small numbers of humans cannot possibly discern. Computers also provide indelible institutional memory in contrast to human analysts who rotate from job to job.

Ambassador Taylor has told the staff that the main problem is not to gather more information, but rather to use the information and technology to mine what we already acquire. Governor Gilmore has advised us that we must link all the databases together. Admiral Wilson, the just-retired Director of DIA, insists that all-source analysts have to see all the data we collect, not just what the agency that collected it decides is important or relevant enough to disseminate. His assertion that the HUMINT and SIGINT databases contain a wealth of useful information that never gets examined is proven by the Mihdhar and Hazmi cases. The joint inquiry has spent an enormous amount of time and effort trying to understand why the intelligence on Hazmi and Mihdhar was not given to analysts and consumers.

What we all have to understand is that still today, very, very few counterintelligence analysts can get access to the databases that held the information on Hazmi and Mihdhar.

Admiral Jacoby, until recently the senior intelligence officer for the Chairman of the Joint Chiefs, insists that analysts, not collectors, must be the proprietors of raw intelligence data, including especially CIA's operations cables, NSA's SIGINT intercepts, and the FBI's terrorist investigatory information. Admiral Jacoby quotes the DCI himself on the need for a fundamental shift in culture and in practice.

On the other side of this position are the arguments that the imperative to protect sources and methods precludes wider access to raw data. NSA also insists that only people formally inside the SIGINT system can see raw signals intelligence due to the need to protect the privacy of U.S. persons. In the case of the FBI, there is the added concern about compromising legal proceedings and ongoing investigations.

I do not see why people outside the CIA should not be allowed to see sensitive HUMINT material provided that these people are subject to the same security standards as CIA employees are. The same is true for NSA. As for the concerns about protecting the privacy, U.S. persons, people outside of NSA can be trained and certified in NSA's so-called minimization procedures. With respect to the FBI, we hope that the PATRIOT Act has already provided the legal foundation to break down the inappropriate barriers to information sharing.

I hope that one of the strong recommendations of this joint inquiry is that all-source counterterrorism analysts must have direct access to intelligence databases and the ability to exploit those databases with modern computer tools.

I would like to ask Mr. Andre and Ambassador Taylor, in that order, to comment on what I have said, particularly with respect to protecting sources and methods, privacy and law enforcement sensitive information. I would also like to ask Mr. Andre this question: Has anything fundamentally changed since 9/11 in terms of who has access to the databases that contained information on Hazmi and Mihdhar?

Mr. ANDRE. Yes, sir, thank you. Thank you for the way you framed the issue. I couldn't have done it better myself. I am very passionate about the role of all-source analysts in this process and believe they have been undervalued and underemployed in this regard and to be properly employed they have to have access to more information.

Let me be clear on a couple of points that maybe are not as clear in our statements as they should have been—that is, Admiral Jacoby's as well as mine—and that is there is not now nor has there been a problem with the sharing of what is deemed to be threat information. Any information collector—I know of no instance where an information collector was anything less than very responsive and very responsible and disseminated that information widely with a sense of urgency.

So the sharing of information from our perspective falls more into the category of the Mihdhar-Hazmi information, which is sort of seemingly benign activities, deliberations, acquisitions, travel by people that wish us harm. It is that information that we wish to harvest.

We don't believe, as all-source analysts, that we have to get access to the source data. We understand completely the need to protect sourcing. We respect that. There are cases where we certainly would want the freedom to go back to the collector and get some evaluation of a source to help our analysts when they are evaluating that particular piece of evidence or those assumptions.

So it is the substantive data, not the circumstances of its collection that is important to us.

Much has fundamentally changed since 9/11. We have a different level of access to data from all of the organizations that you mentioned, CIA, FBI and NSA. Some of the inhibitions on us getting information reside with us. We have taken a lot of measures to change the way we do business so that the information provider can have a greater degree of confidence that we can be trusted with their data, and of course our job is to show them not only can we be trusted but we can add value to that information.

We have taken a real hard look at some of the documents that are used to tell us why we can't have certain information. For example, in the signals intelligence area, Executive Order 12333, I am not a lawyer, but I have had a team of lawyers look at it. That document is a very powerful document that compels sharing of information, not withholding information. We are very optimistic that things are in train to dramatically increase the level and type of information that is shared.

Ambassador TAYLOR. I think when I spoke to the staff on this matter I was reflecting on the time I spent on active duty with the United States Air Force as the head of its investigative organization, OSI, and in that position it became clear to me that our inves-

tigative community, our counterintelligence community, indeed our counterterrorism community, needs to view information in a different light.

Investigators historically look at information as it relates to the case that they are working on, and that becomes their focus. It is how we are trained, it is how we focus for prosecution, arrests and so forth and so on. But it also became clear that there are nuggets of information in those investigations that affect more broadly our Air Force, and that one agent that is conducting that case cannot have the perspective to understand that without sharing that information more widely within the community.

Mr. BISHOP. Without analysts?

Ambassador TAYLOR. Not solely without an analyst, because analysis is one part of the challenge. The other part of the challenge is enabling others who are part of the reins of security that we have, for instance, the Customs officer in Seattle that stopped Ramzi Yousef, who is also a key person, not to do analytical work but to understand that this particular individual, someone in the U.S. government, knows something about this person that he or she needs to check out.

So the challenge is to place into the information technology system the ability for our analysts to get access to things that they need, but also to give to our first responders, to our security officers, to our INS border guards the information they need, which is not the same as the information that our analysts need. Our border guards need to know that Frank Taylor is a person of interest, and therefore we need to check him out. Our analysts may want to know a lot more about what Frank Taylor has done.

I believe information technology can help us to do this. There is a very real concern with sources and methods. We have to protect those sources and methods, because, without that, we will never have the information. But I don't think that is insurmountable in triaging the information and providing it in the appropriate channel with the appropriate classification to the people who need it to bring more clarity to the picture, the counterterrorism picture.

Mr. BISHOP. Thank you. Admiral Jacoby's statement for the record as well as the statement from the General Accounting Office stresses the difficulties posed by incompatible database structures and formats, a problem that afflicts all levels of government across the board.

This incompatibility makes it hard to share that across agencies or to conduct analysis across all of the government's diverse databases. The GAO and DOD statements explain that that is a viable alternative. The private sector has settled on a common data framework and a set of standards that allows full interoperability across organizations. This capability is as essential for industry in the electronic age as it is now for our government in the war on terrorism. But our government is way behind the private sector.

The commercial standard is called XML. Testimony before us today illustrates how important it is in the war on terrorism for the government to adopt this standard and to move quickly to convert our existing databases. Adoption of XML not only allows full data sharing, it also offers much more effective and efficient ways to analyze data and to automatically update files.

Here is another instance where I believe action by the two intelligence committees is warranted now. We could mandate adoption of XML and give the Intelligence Community a date certain by which it would need to have shifted over to the new standard.

Mr. Andre, how difficult would it be for DIA to shift over to the XML standard? Do you think that it is practical to insist that the Intelligence Community as a whole shift to this database standard and do it rapidly?

Mr. ANDRE. Yes, sir, thank you. Let me say a major investment that we have made in the Joint Intelligence Task Force for Combatting Terrorism is transitioning their entire data environment into an XML environment. We think it is exceptionally important for the reasons you pointed out.

One of the most important aspects of that is the ability to tag at the content level rather than at the record level. We believe that ultimately if, like the commercial sector, the Intelligence Community adopted the XML approach, that data—they don't have to reside in a single repository—we can have interoperability at the data level and really empower that data and be able to do things with it we can't today.

We are a pretty good test case in both the JET FTS and the J–2 part of DIA, because we are also transitioning the J–2 part into a fully digital XML environment, changing the way we produce products, using, I might add, off-the-shelf commercial technology. It is not easy. It is painful. I guess the big question is, I think it is a lot simpler to sort of go from a standing start and say from this day on I am going to be in an XML world, rather than to say I have got 40 years worth of great big databases like the military integrated database and I have to convert all of that data, properly tag it. It will cost a lot of money, it will take a lot of time. But the end result will be certainly worth it.

Mr. BISHOP. Thank you. According to inquiries by our staff, the FBI contacted both the State Department's Bureau of Diplomatic Security and INS in August of 2001 about Hazmi and Mihdhar. Both agencies possessed information that would have helped locate the two suspects but the FBI asked for specific information and nothing more and expressed no particular urgency about finding them.

Both agencies claimed that they had ways of finding the two and could probably have done so if they had been asked. Could the State Department or INS witnesses please explain how their organizations could have located these two suspects and could they provide any insight on why the FBI did not explain why it was looking for them and why they didn't request help?

Ambassador TAYLOR. I will go first, Congressman. Certainly we were informed in August by a request from the FBI for visa records on both of those individuals, and that is a routine request that we get very frequently, and we responded to that request, as we often do, not asking the reason for the inquiry. The FBI runs thousands of investigations where that data is necessary.

Today that would not happen. We would ask that question, given the benefit of 20/20 hindsight.

In our responsibility to investigate visa fraud, we work with many data companies around the world to—around the country ac-

tually—to look for individuals that we suspect are involved in visa fraud. Most recently we have had a major investigation involving that, and we were able to locate 39 of 72 suspects in about a month. We have the capacity to do that. We know how to do that, but we were not asked to do that. Today we would ask that question and we would volunteer our assistance to the Bureau if they were indeed looking for those individuals.

Mr. GREENE. Yes, sir. From the INS point of view, not only do we have a variety of other databases that contain information, people who would apply for benefits under immigration law or people who would travel in and out of the United States that might provide us with some leads, the Law Enforcement Support Center, as I mentioned in my statement, also has access to a variety of criminal databases and also private sector databases that we can then mine to use as potential leads for an investigation.

It is not unlike what we did during the first Absconder initiative last spring. So I think the capability is there certainly for us to have made a contribution in terms of actively—had we been asked, to actively seek this person, to take a good shot at going after them and locating them.

With respect to the motivations behind the information that we received, I simply can't answer that. But certainly from the standpoint of having capabilities, we believe we could have brought some to the question.

Mr. BISHOP. I think my time has expired. Mr. Chairman, let me thank you and thank Senator Wyden for deferring to me because of the exigencies of my schedule today. I thank you very much for that.

Chairman GRAHAM. Thank you, Mr. Congressman. Best wishes on the floor of the House of Representatives today.

Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. I thank Congressman Bishop for his excellent questioning.

Gentleman, I come to this with the view that our software and search engines and data mining tools can go a long way to beating the terrorists, but we just are not using what we have got, because we have got all these separate government fiefdoms in effect running databases strewn all over Washington, D.C., and they have either been unwilling or unable to get together so they are connected and then give us the best possible strategy to pick up dangerous trends.

To change this, I wrote legislation—it is now in the intelligence conference; we are working on it now—that would create a single database where all U.S. information on terrorists from the Intelligence Community, other Federal agencies and State and local officials can be gathered together and shared with any intelligence or law enforcement official who needs information on suspected terrorists.

What this ensures—and Commissioner Norris, I think you summed it up—this ensures that everybody is on the same team, Federal, State and local. I hear it from law enforcement officials in Oregon. You have echoed it again. You are not going to win the war on terrorism from Washington, D.C. Much of the important work is going to have to be done at the local level.

The reason I bring this up this morning, Mr. Chairman, is, with this item in conference right now, I hope that what we have heard from these six very good witnesses will give us additional strength in terms of getting that terrorist identification-classification system properly funded in the conference. It should be decided, as we all know, very shortly. Gentleman, I think you have given us some very helpful information to get that properly funded.

Let me begin my questioning, if I might, with Mr. Manno. The TSA Office of Civil Intelligence is formerly the FAA's Intelligence Division. I wanted to begin with you and particularly some of the history.

There are years and years of history beginning in December of 1994 with the Algerian armed Islamic group terrorists, their hijacking the Air France flight in Algiers and threatening to crash it into the Eiffel Tower; the 1995 evidence that came from the Philippine national police raid, turning up materials in the Manila apartment talking about crashing an airplane into CIA Headquarters. There is years and years of history with respect to the proposition that terrorists are willing to use airplanes as the tool to carry out their agenda.

Given that—and my understanding is that FAA at that time had some of that information—why wasn't it used to put in place a comprehensive set of new security procedures so that, for example, let us say, in the late 1990s, by the late 1990s there could have been a requirement for hardening those cockpit doors. Why wasn't that information that was developed in the beginning, in a serious way in 1994, used to put in place tough new security procedures by, let's say, the late 1990s?

Mr. MANNO. Well, Senator Wyden, we started to take a real close look and perceived the change in the threat environment dating back to 1994. In fact, we worked very closely with the National Intelligence Council and asked for and received a threat assessment, a national threat assessment, that was produced by CIA and FBI, and at that point actually invited in for classified briefings a wide range of representatives from the aviation industry and airports, associations like the Air Transport Association, in order to explain to them the threat had in effect changed from what it was previously, specifically with respect to some of the radical Islamic groups that appeared at that point to be in this country.

That effort, our ability to actually provide classified briefings, ironically enough the briefer from the FBI side of the house, because the briefing was actually presented by CIA and FBI officers, was John O'Neill, who subsequently perished in the World Trade Center.

Based on that, there were a number of measures that were implemented that changed what was the baseline security measures that had been in effect at that point.

In the case of the industry, there is always a desire to know why the regulatory agencies, in this case FAA, are requiring additional measures, because those things cost money. So that effort, with the help of the Community, helped us to convince them of the change in threat. There were a number of specific things that were in fact done.

Senator WYDEN. At that point, did you go to the industry in, say, the late 1990s and say we need changes like hardening the cockpit doors and they were unwilling to support that?

Mr. MANNO. What we do with the industry, there is an ongoing effort to keep them apprised of the general threat, of changes in the threat, in changes of MOs by terrorist groups, and we have done that in a number of different ways, either through the unclassified information circulars and directives that we sent out, the briefings that we have conducted for them, even to the point where we produced a CD that was disseminated to over 750 elements throughout the industry that spelled out in great detail what the threat was, the fact that it was changing. In fact, it even mentioned the possibility of suicide attacks.

Again, this was something that was not based on any specific information that we had received from the Community that indicated that these terrorist groups were in fact planning something like this, but it was a notion that it was a possibility.

Senator WYDEN. With respect to al Mihdhar and al-Hazmi, did your agency have the names of those two hijackers prior to September 11, 2001?

Mr. MANNO. No, we did not.

Senator WYDEN. If you had, what steps would have been taken, had you had that information?

Mr. MANNO. Well, prior to 9/11, we had a process, we had a so-called watch list which was disseminated to the industry via the security directive process. In fact, a number of the people that we suspected were involved in what we call the Manila plot, the Bojinko plot, as you referred to it, were on that list. Again, what we would—the purpose of that process was to highlight for the air carriers particular individuals, individuals that had ties to terrorist groups and that presented a threat to aviation who should either be denied boarding or should be, if they showed up for the boarding, called to the attention of law enforcement.

Had we had information that those two individuals presented a threat to aviation or posed a great danger, we would have put them on that list, and they should have been picked up in the reservation process.

Senator WYDEN. Is your intelligence office connected to the major watch list, like TIPOFF?

Mr. MANNO. We now have access to TIPOFF through IntelLink and CTLink.

Senator WYDEN. Has your office ever had direct access to the National Criminal Information Center data that is maintained by the Department of Justice and the FBI?

Mr. MANNO. Currently we don't, but we have liaison officers that are posted to CIA and to FBI where they sit side-by-side with other officers from INS and Customs, so they are able to access it that way.

We are also in the process—we are in the negotiations with the Customs Service to get access to their text system, with a terminal that will be placed in our intelligence watch, which will then give us access to NCIC. So we have in-depth access to NCIC through our liaison officers and hopefully soon we will have it directly.

Senator WYDEN. Does your agency believe that when there is intelligence information related to a potential threat to civil aviation, that you are now getting unfettered access to all of the intelligence, including the raw intelligence?

Mr. MANNO. I don't think that there is any question in the minds of the agencies that produce the intelligence that if this is specific threat information that we need to act on, that that is provided to us. I think what we may still not be receiving is what Mr. Andre alluded to before, is the background information that would help our analysts in better understanding the threat environment. We do that to a great extent now in producing threat assessments. The analysts that work in our Office of Intelligence come from the Community. We hire them from other agencies, so they bring that perspective. That has helped. That kind of information would in fact help us do our job better.

Senator WYDEN. Let me ask you specifically about the Phoenix memo, obviously the memo where the FBI agent created an analytical product detailing suspected terrorists seeking flight training. When did your office first see that Phoenix memo?

Mr. MANNO. The first time that we saw it was when it was brought to our attention by the committee staff when they came to visit us.

Senator WYDEN. When was that? Is it correct you first saw that memo even after congressional hearings?

Mr. MANNO. The actual memo, yes. We did not see it until the committee staff brought it to our attention.

Senator WYDEN. When was that?

Mr. MANNO. I don't know the exact date. We can get that for you though.

Senator WYDEN. But I am correct in saying that you did not get to see this memo, which many of us felt was an enormously important message, you didn't get to see it, not just before September 11, you didn't get to see it until after congressional hearings were held looking into this issue, is that correct?

Mr. MANNO. That is correct.

Senator WYDEN. How would your office have responded to the Phoenix memo if you had received it prior to September 11, 2001?

Mr. MANNO. I think we would have started to ask a lot more probing questions of FBI as to what this was all about, to start with. There were a number of things that were done later to try to determine what connections these people may have had to flight schools by going back to the Airmen Registry in Oklahoma City that is maintained by the FAA to try to identify additional people. In fact, that is what goes on right now. The law enforcement agencies, of course, have access to that database, and whenever we on an ongoing daily basis, whenever our watch——

Senator WYDEN. Would you have treated that as priority business? In other words, would you have stopped other business to go after that?

Mr. MANNO. We take all threats seriously. In fact our process is whenever we get a threat, we open what we call an ICF, an intelligence case file, and that is so we segregate that issue from the hundreds and hundreds and hundreds of other intelligence reports that we get and that we focus on it. And the work that may entail

in trying to determine whether this is a credible threat, something that needs to be acted upon, may be going back and working with FBI to try to get additional information. In some cases it can be working with the State Department or the CIA if it requires overseas work. So we make all efforts to try to get to the bottom of what this is all about.

Senator WYDEN. What recommendations have you all made regarding suspect flight training and have any of those recommendations been implemented since after September 11?

Mr. MANNO. There are a number of things that have been done. There was an effort to sensitize flight schools and fixed base operators that rent aircraft to report suspicious activity immediately to law enforcement agencies. These are the people that can best identify whether somebody is seeking training in their schools or seeking to rent an aircraft. That's the best chance that we have that somebody like that will be identified and reported to law enforcement.

There also is an effort actually by the Justice Department to vet people from other countries that seek to come to this country to obtain flight training where they will have to in essence undergo a background investigation before they are actually allowed to take training.

Senator WYDEN. I am going to move on to question some others, Mr. Manno, but I want it understood that with the FAA getting the Phoenix memo in early May this year, 2002 and the FBI agent having written it in the summer of 2001, I don't think there is a more graphic example of how dysfunctional this system is and this is what has got to be changed. And we are going to try to do it with a terrorist identification classification system. I think some of the examples you have given us today are very helpful. But this example is what the reform agenda has got to be all about. You can't explain that to the public that something that important, that significant was available in the summer of 2001, didn't find its way to your agency until May of 2002.

I am going to move on, but, Mr. Chairman, this is something I feel very strongly about. We are going to jump on the terrorist. This is the kind of information that has got to make its way through the system.

Ambassador Taylor, if I might turn to you on the question of needing more personnel, which is something that has been touched on several times this morning, do you need more personnel to process the information that you receive? Is this a question of personnel or lack of technology? Tell us what you think the challenge is.

Ambassador TAYLOR. You are speaking in terms of the information we receive within our visa system or more broadly?

Senator WYDEN. Right. The information you need to get through, and certainly you've touched on the major areas.

Ambassador TAYLOR. We have made a major investment in technology and will continue to make that investment in technology. We do require interface with the Intel Community to broaden, perhaps, the TIPOFF data base. We have now been funded for that purpose and certainly should that be the case, I think our Secretary has had discussions with Director Tenet on that issue and would look for a collective effort with the Director to expand the

TIPOFF database with other data from CIA databases. I am not in a position here to tell you that I need X number more people or X number more dollars for technology, except to say, sir, that we are focusing very squarely on this need. We just completed our 2004 budget review with the Deputy Secretary. I think he believes very strongly he will reflect those priorities when that budget comes forward, and our Department has no higher priority than to focus and improve on our system and the availability of our system to other members of the Federal, State and local government.

Senator WYDEN. Governor Gilmore, question for you, and we have enjoyed working with you over the years. As you know, I chair the Science and Technology Subcommittee as well and enjoyed our relationship. Tell me, if you would, what major recommendations did your advisory panel make that have yet to be fulfilled by the administration, the Congress and other governmental bodies?

Mr. GILMORE. Most of the recommendations that we have made have, in fact, been adopted. We have made about 80 or so, Senator Wyden. I think where our focus is right now is on what we're going to be doing in this coming report in December. And on that we are going to be focusing on the need for a unified fusion center for the purpose of bringing together information from all sources.

The emphasis on the questioning today has been on the exchange of information through databases. But our focus has been on the cultural changes that need to be made. And we will probably recommend a fusion center, a stand-alone, independent organization that would be in a position to bring information together from all different sources and pull it together. With respect to other recommendations that have not been made, have not been at this point implemented, we don't believe there has been a sufficient focus by the Federal Government on the necessity of working together with States and locals, particularly the exchange of information.

For example, we have suggested that there be major procedures and processes put into place in order to share important information even after analyzed, Senator, with State officials, Governors and then key officials in the localities. Nothing like that has been done nor hardly discussed. Even now most of the discussion is among the Federal agencies and the exchange of information as opposed to the true creation of a national strategy.

Senator WYDEN. Let me see if I can get one last question in. Mr. Andre, the former DIA Director, Admiral Wilson, has told the joint inquiry staff that he was never sure that he received all the available intelligence information. He also said that senior defense officials received information that his analysts did not receive and he questioned what good in effect it did for him to be aware of intelligence information that his analysts did not receive.

So my question to you is, what impact prior to 9/11 did the withholding of some intelligence information from analysts have on the DIA's ability to do the kind of all-source analysis that's needed to do the job properly?

Mr. ANDRE. That's a tough question because we don't know what we don't know. But it brings up a point, particularly the issue of information going to very senior officials and not to the analysts.

You notice in my statement I talked about information that was not subjected to analytic scrutiny. I think that's the key. We are pleased when a collection agency whispers in the ear of the Secretary of Defense or the Chairman of the Joint Chiefs of Staff or the Director of DIA, and that's good. However, to extract meaning from that data, to perform the true analytic function, we need to get that information into the hands and the brains of analysts who are paid to fill in the gaps of missing information to compensate for absent evidence and to turn information into knowledge. That's what we pay them to do. They don't have the information, they can't do that. So it's hard to judge what the impact of missing information was, except to say categorically that our knowledge thus was incomplete.

Senator WYDEN. Chairman, thank you.

Chairman GRAHAM. Thank you, Senator. Thank you for excellent questions and the informative responses of the members of the panel.

Congressman Hoekstra.

Mr. HOEKSTRA. Thank you, Mr. Chairman, and thank you to the panel for being here today. I guess I am not buying in yet that things have improved all that much since September 11. If you go back through the history, it appears that information-sharing has been a long-term problem. The bureaucracies have put in a number of different mechanisms to try to deal with that over the years—signed memoranda of agreement with other agencies, the use of details employed to other intelligence in law enforcement agencies, participation in joint task forces, attempts to design and field common databases. Governor Gilmore, in your work of your committees, have you gone back and taken a look at how long information-sharing has been a problem in these different types of mechanisms and their effectiveness in improving the situation?

Mr. GILMORE. Congressman, I don't think we're buying it either. We think that much more needs to be done in order to be able to share information. We were alert to it when we began our commission back in January of 1999. We began to inject it into our reports, which of course were submitted to the Congress and to the President. Again, ladies and gentlemen, we are a congressional advisory panel. We are established by your statute and we have been here to give you this information and we have been very happy with the Congressional attention that we've received and hopefully we've been of help to you.

With respect to this issue, though, it's been true from the very beginning. I think, Congressman Hoekstra, I would make this point and I think we have made this point in our commission. The challenge is not so much technical and even good wishes of people that want to meet together on task forces and so on; there is a cultural difficulty that we have to confront. And the cultural difficulty is that organizations that gather intelligence don't share that information. They don't share it because of turf issues, because of, frankly, the system that we've always had of holding things secure. And if you give it out to somebody else there's a risk that it will be released and as a result we have cultural institutional resistance built into this, and I think that is what has to be confronted.

Mr. HOEKSTRA. Can you explain to me how the fusion center will work in a way to address those issues so that if a joint committee is sitting here in two or three years, it's not the fifth one will be a fusion center, another failed attempt at, you know, information and data sharing? What makes the fusion center a solution rather than another Band-Aid?

Mr. GILMORE. The theory under which we are working and beginning to develop for our final report would be that you would begin to take counterterrorism information from all the different intelligence agencies and put them in one place where a group of people can look at it from that basis, instead of it being ad hoc, instead of being separated out through this culture of separation and lack of information. Put it together in one place and give one body of people a chance to look at that and that would facilitate the opportunity, not necessarily the conclusion but the opportunity for communication with States and locals as well, and they need to give information and get information. Quite frankly, much of the information of what's going on in the communities out there, suspicious activity and so on, isn't even in the Federal Government. It is in State officials and local law enforcement people.

Mr. HOEKSTRA. Ambassador Taylor, you talked about in your testimony or in the interviews that you've given to the joint staff, you talked about the ability perhaps to help the FBI. Why would it be that in the year 2001 the FBI would not have seen your resources within the Department of State as being a significant asset in helping them find these individuals that they put on the watch list?

Ambassador TAYLOR. I don't know that the FBI doesn't see our resources as a significant help to them. I suspect that in this particular case an agent was following the leads that he was given and didn't see a need at that time to ask for that assistance. I've learned over the years that in the investigative community sometimes we don't realize how much capability is out there to help us until we ask, and experience goes a long way in learning who can help you get these things solved. So I don't know there is a reluctance by anyone in the FBI to do it. It may just be that the individual asking that question didn't understand how we could be brought to bear to help them solve that problem.

Mr. HOEKSTRA. So they didn't understand your capabilities or they do understand your capabilities? Because earlier you said that you would now ask the question—you would now ask the FBI the question. You wouldn't just receive the information and say okay. We have now asked them the question. If there weren't any urgency or whatever, you'd probably get the same response and don't worry about it and just go through your normal procedure and don't put it on priority. Is that what you would have expected to happen?

Ambassador TAYLOR. Well, today we would ask the question why are you asking us for this information because of our responsibilities for visa fraud and should we be joining you in this effort that you are engaged in? Indeed our agents that are now at the 19 joint terrorism task forces, their primary reason for being there is to make sure that when inquiries come up involving visas in a terrorism investigation they are there and available to help support

the investigation, not as an afterthought but as an integrated part of that investigation.

Mr. HOEKSTRA. Commissioner Norris, both before the hearing and in your testimony, you indicated a level of frustration that perhaps you may have seen some improvement but it's not anywhere where you think it needs to be for you to do your job effectively, is that accurate?

Mr. NORRIS. That's quite accurate.

Mr. HOEKSTRA. You're not buying it either?

Mr. NORRIS. I'm not buying it all. Governor Gilmore is right on the money. The discussions we have been hearing for the last year, it's been frustrating to me and others in my position because most of the discussions they just don't get it. There's a lot of discussion about the technology and access to databases. This is not—it's not the way to do it.

What we are looking for, a fusion center, intelligence center, something like that, because frankly as much as we need the information to be given to us, because you know we learned about the Orange Alert the way everybody else did in America, on television. And we need to know not only why we're at this level of alert—that we are, but why we are. Do we look up? Do we look down? And the fact is, as was just stated, we're the biggest gatherers of intelligence in America.

In my city alone we arrested 100,000 people last year. We stopped 235 people who were given receipts called stop tickets. We took their identification. We know who they are, where they live, what car they were driving, what they said. We have many narcotics investigations. We have wiretaps up all over the city. We have cameras and intelligence cases going. We can't share this with anybody who needs to see it. And frankly, we're the biggest collectors. It's not the Federal Government. We want to give it away and we can't. The fact we can't give this away is frustrating because we can tell when people move from one cave to another in Afghanistan, but we can't tell when they move from one row house to another in Baltimore. If someone's wanted in Florida, wouldn't you like to know he was stopped in Maryland for a traffic stop, was arrested and given a ticket because he was suspicious by local police? This information is out there and no one is looking for it.

Mr. HOEKSTRA. What information do you have or receive on the different Federal databases that are out there and available? Are you sometimes surprised that the databases—that maybe if you are watching a hearing or participating in a hearing, saying I didn't know the information was available?

Mr. NORRIS. Sometimes we don't know it's available. The frustration sometimes though is that you know as investigators we are looking beyond the horizon. When we see things that are suspicious to us, we want to go further in our investigations. And what's frustrating to us many times is the tendency to figure out the reasons why we call this a terrorist investigation or there is no reason to look at this any further when the fact is we should be looking even further when you got stuff that I discussed in the beginning and not figuring every reason why we should be discarding this.

One of the things asked me by the local media when we uncovered this group of people who may or may not be a support cell or

an operation, I don't know what they're doing, but their statement to me was, well, they are not on anybody's watch list. Oh, you mean the list that bin Ladin is going to provide to the American government of people who were here for the last 15 years. It's a ridiculous proposition. We need to be looking at everything that's being worked on around this country. We have had people photographing and sketching the Inner Harbor in Baltimore. We brought them in. They are in Federal custody now. Some are being deported. Shouldn't the police in New York know about this, and Philly and Boston? Wouldn't they all like to know just in case they had similar activity on the same day, which in our case was the 4th of July.

This is the stuff we need to be sharing, and it's not going to be done by database. It's going to be done by us talking to each other sitting in a room over coffee because that's how our work is done in law enforcement. If you're not sitting there every day talking to each other and discussing yesterday's events, it's not going to happen.

Mr. HOEKSTRA. I am not sure whether the answer is—something along the lines like Senator Wyden has proposed or that the commission will propose from Governor Gilmore—but I believe another Band-Aid approach in 2002 is not going to be sufficient. And Mr. Manno, it is not your responsibility, but let me just send a message because we apparently can't get calls returned from TSA, but you know, if you're dealing with other agencies, if TSA is dealing with other agencies in the same manner that it is dealing with perhaps some Members of Congress and for your customers, the people that go through your screening at the airport, it's business as usual and it's not a learning organization that is trying to improve the way that it deals with—in the airport that I go through, which is a test site for the implementation of Federal takeover of the airport, it has been very disappointing, the willingness—there's some very unfortunate circumstances. The response from TSA to take a look at these opportunities and say, you know, this hasn't worked very well and, you know, we really would like to sit down and interact with the folks who have experienced this so that we can become a better agency to serve the public better, the response from TSA—and again you're the person here and it's not your area of responsibility but this is the only way I can send the message—is that it's disappointing and it says to me this is an agency that is working more like old bureaucracy than new bureaucracy.

Mr. Greene, we are talking about information-sharing. How many undocumented illegal aliens do we have in the United States that we don't have much information on, if any?

Mr. GREENE. I think the commissioner has testified in the neighborhood of seven million.

Mr. HOEKSTRA. Governor Gilmore, does that worry you?

Mr. GILMORE. It's a lot of people.

Mr. HOEKSTRA. I think what we need to be taking a look at is we've got some other issues here. No matter how good we get at information-sharing on the people in the database, if we get to be very, very good at, you know, connecting the dots of the people who are in the database, there are a whole lot of folks—there are a lot of ways to slip into this country which are outside of the databases

and that somewhere within Congress—and I would guess is part of the national strategy on against terrorism—we are going to have to acknowledge that and we are going to have to find a way to deal with, you know, up to seven million people who have entered the country and have gotten here illegally.

Chairman GRAHAM. Excuse me, Congressman, I apologize for interrupting. This will not come out of your time, but there is a vote under way in the Senate. We have approximately six minutes left. So Senator Shelby and I are going to have to leave for that. Senator Shelby has asked if he could commence his questioning when we reconvene at 2:00 this afternoon.

So I will turn the gavel over to Congressman Goss to conclude the morning session and we will join you at 2:00.

Mr. HOEKSTRA. The final issue I wanted to address, Ambassador Taylor, is due to the increased threats to Americans in the late spring and early summer of 2001 and the Taliban's provision of sanctuary to UBL and al-Qa'ida. A demarche was issued by the State Department to the Taliban asserting that we would hold the Taliban responsible for any attacks on Americans by UBL terrorists after that time. In a letter to the State Department on June 18, the Joint Inquiry Staff Director requested that demarche but we have not yet received it.

Can you give us information as to why we haven't received that document and what response you have received from the Taliban?

Ambassador TAYLOR. Certainly, sir, you are referring to a demarche that was delivered on the 29th of June by an ambassador in Islamabad.

Mr. HOEKSTRA. What was the content of the demarche?

Ambassador TAYLOR. Essentially as you have outlined it. We were very much concerned about indications of terrorist planning coming from bin Ladin and al-Qa'ida in Afghanistan and that we would hold the Taliban accountable—excuse me, responsible for any terrorism planned or executed by al-Qa'ida from the territory of Afghanistan. The response in general was that the Taliban were looking for evidence that bin Ladin had indeed been involved in such activity. They did not believe that he could threaten the United States from Afghanistan and they indicated they had no evidence to support our concern.

Mr. HOEKSTRA. You received a written response from them as well?

Ambassador TAYLOR. I can't recall whether it was written or verbal. There was a written response that was translated, but my colleague tells me quite confused. That request is in for declassification, I believe, and as soon as that decision is forthcoming, very shortly that cable will be provided to the committee.

Mr. HOEKSTRA. Mr. Chairman, that concludes my questioning. Thank you very much.

Chairman GOSS [presiding]. Thank you very much, Mr. Hoekstra. I understand Ms. Harman would be recognized for five minutes now if she chose. The gentlelady from California.

Ms. HARMAN. Thank you, Mr. Chairman. I want to apologize to the witnesses for missing their testimony, but as Governor Gilmore knows in particular, this subject of information-sharing or the lack of it is much on my mind. I want to say to you, Governor Gilmore,

I think you get all the prizes for chairing the most commissions that have done the most work on the subjects we have been addressing in this joint inquiry. I was a member of one you didn't chair. It was ably chaired by Ambassador L. Paul Bremer, and we made some recommendations as well. I am pleased to hear that most of your 80 recommendations have been adopted. I think that is a good start. Many people out there were talking about changes. But I think, as we have just been saying, that much more needs to be done.

I want to ask about one idea that has passed the House by a bipartisan vote of 422 to 2. That is unusual, as we all know, and maybe a good model for future votes, but at any rate, another member of this committee, Saxby Chambliss, and I introduced an information-sharing bill which did pass the House. What it requires is for a program to be developed by the administration within, I think it is now a year—we had initially proposed six months—to share information in a redacted form with sources and methods deleted over existing networks like the NLETS network with our first responders.

I know this won't solve the whole problem, but I did want to get on the record your response to this approach. It has broad support from outside as well as inside. Governor Ridge's office is in support of it, for example. And somehow we haven't yet gotten any momentum going in the other body.

Unfortunately, no Member of that body is sitting here. They are all voting, but I would like to make a record on this subject and perhaps you, Governor Gilmore, first and any others to comment during my five minutes. And by the way I wish you good luck in your new law practice.

Mr. GILMORE. Thank you, Congresswoman Harman, and thank you for your leadership.

Congresswoman, I have been working on these issues several years now and we appreciate your leadership. With respect to this issue, one of the central tenets of the commission's reports that we have submitted to the Congress and the President has been the necessity of a national strategy that includes Federal, State and local personnel. As we have said today in this testimony, it is absolutely essential that we utilize the strengths that exist in the first responders and the States.

The theory under which we have been operating as the correct way to respond is to the utilization of the first responders and having them trained, financed and prepared to play that role. Under a State plan and with the support of State organizations, particularly with the emergency operations centers established in the States, which is the model we see all the time, it works on floods, disasters of different measures and it works very well, usually in partnership with FEMA, the lead Federal civilian agency, and with all of this that this is a good response. With respect to prevention, you cannot prevent without the sharing of information.

Congresswoman, if your system could go into place to put at least some structure into place to get information into the hands of the first responders and the States that organize and manage the overall State responses, that would be a tremendous asset, and then

from there we could always find ways to refine as we went along. But first it would be great leadership if it could be established.

Ms. HARMAN. Thank you. I think I would love to hear from the Admiral.

Mr. NORRIS. I've been promoted.

Ms. HARMAN. I'll promote you to anything if you can solve this problem.

Mr. NORRIS. We would be very much in favor of what you just proposed. Very frankly, we hear so much discussion of sources and methods and the protection of this. If the information coming was overheard in the coffee shop in Turkey or from a paid informant in London, it's of no importance to me. We just need the information. We are charged with protecting our cities and right now we are not getting any information to do so, and it has not gotten any better a year later. And if we could get information into our hands and get it in quickly, we certainly would take it in the redacted form, we would be very much in favor.

Ms. HARMAN. I think my time is up, but I would just comment that it answers the problem you posed, which is we need to know what to do. It's not just the need to know to be alert. It is what should you do and you need actionable intelligence that can direct you to people or places to find people or protect places, and this is the kind of thing that could be transferred through the system. And I would just urge our witnesses and others hearing my comments to suggest to the Members of the other body that they might attach this idea to the homeland security bill or pass it as an independent bill so that we can get action as quickly as possible. I think this is sorely needed. And in fact, my understanding is the administration has the authority to do this without legislation. So maybe this suggestion will fall on friendly ears and this policy will be enacted even without legislation.

Thank you all very much. Thank you very much.

Chairman GOSS. Thank you, Ms. Harman, I am going to use my five minutes in the interest of abbreviating the afternoon session if we can hang on for five more minutes, and then we'll break for lunch. My questions go specifically to statements you have made in your very helpful presentations to us, and I want to thank you all because I think you have all emphasized concerns that we have that are legitimate and indeed need attention and frankly we have learned some new and interesting thoughts.

Governor, I would like to ask you first of all, if you can explain to me why all the brilliant work that you and your panels did with Ms. Harman received the same audience reaction that the work that the House and Senate Intelligence Committees received on the subject of threat warning during the end of the 1990s and into the 2000 Millennium?

Mr. GILMORE. Mr. Chairman, I think one needs to go back to where this was at the beginning of 1999, when we were formed. The Congress was expressing concern. That is why the commission was formed. The commission is not a typical Beltway commission. It is not a group of wise men. It is heavy on—chaired by a State official, a Governor, general officers, retired, are on this, intelligence representatives, but very heavy on fire, police, emergency services, health care, epidemiologists and all drawn from the States

out in the communities to get a different sort of look, and that is what the Congress was looking for.

But at the time, you know, it's hard to go back and think before 9/11. It was just a searing experience, but it was considered to be somewhat theoretical. It was considered to be something that people were concerned about, but there was no imminent threat being defined by any law enforcement agency anywhere. So as a result, we were putting together the best information we could based on the information we had working with the RAND Corporation in order to determine that there were threats, but we are in a position only to say what we had thought from a matter of policy.

It isn't the same thing as an alert. An alert has to be based on hard intelligence gathered from intelligence organizations from all levels of government, synthesized and put together in order to issue a real warning in the right place. And that I think would get people's attention on an operational basis. But meanwhile in the early 1990s, this was a policy group and remains a policy group making recommendations to the Congress and the President.

Chairman GOSS. Commissioner Norris, if I may ask you two specifics. One is your capabilities with your law enforcement people. Do you have a language capability in your analysis center is the first question, and the second question is are you restricted, your law enforcement personnel, from going into public places like mosques, churches and so forth?

Mr. NORRIS. We do have a language capability, just by good fortune. One of the sergeants in my intelligence division speaks Farsi and Arabic, and we have others with the same language skills. They were drafted into service there. We are fortunate in that regard.

Chairman GOSS. Do you think that is unique or in other cities around the country?

Mr. NORRIS. In the NYPD, I know they have tremendous language skills just by the sheer size of the organization. I think it is kind of unique. We have it because, frankly, the Federal agencies have been asking us for assistance in that regard because we have native speakers who become police officers. So we were very fortunate. As far as the mosques, it's a pretty sensitive subject in most cities, including ours, and intelligence is a dirty word. And police agencies, for a long time we have a criteria of opening an investigation of cases and the like, and that's how we get into these places before we put any of these people in as undercovers. We get information from all communities, from community members, meetings, community affairs. But as far as placing undercovers, it requires obviously my approval.

Chairman GOSS. Is it policy or is it a question of law?

Mr. NORRIS. It's a question of policy right now.

Chairman GOSS. Last question would go to Mr. Greene. You mentioned Florida and the working relationship that is being initiated. Is it your assessment—I know it's early and I know a couple of the individuals involved, Sheriff Hunter and some of the other people you have worked with—is it your opinion that this is working or not?

Mr. GREENE. I have the strong sense that it is. We have gotten some feedback from our own people who are working with the local

law enforcement agencies that this is a good partnership. There's one arrest that we can report, and I can give your staff the details. But by and large, the biggest boost for us is the fact that we are working side by side with local law enforcement agencies on these domestic security issues and, as the commissioner described it, the interchange over the coffee is the force multiplier for us.

Chairman GOSS. We would be glad to provide more coffee. Thank you very much. We will be at luncheon recess until 2:00, at which time Chairman Graham will return and I understand Senator Shelby will start with the 20 minutes of questioning. I wish you a happy lunch.

[Whereupon, at 12:45 p.m., the joint committee was recessed, to reconvene at 2:00 p.m., this same day.]

Chairman GRAHAM. I call the hearing to order.

Senator Shelby is the next 20-minute questioner.

Vice Chairman SHELBY. Thank you, Mr. Chairman.

Mr. Chairman, first, I have got a statement to make; and then I will get into the questioning. I know some of the panel have got a time limitation. I will try to be brief.

The topic of information-sharing has become a central theme of our investigation, as everybody here knows. I believe there is now unanimity on the need for our government, yes, our government, to consolidate and to manage all, all available information on the terrorist threat.

Most Americans will probably be surprised to know that, one year after the terrorist attacks of September 11, there is still no Federal official, not a single one, to whom the President can turn to ask the simple question, what do we know about current terrorist threats against our homeland? A year later, no one person or entity has meaningful access to all such information that the government possesses. No one really knows what we know, and no one is even in a position to go to find out as of the time we are sitting here.

This state of affairs, I believe, is deplorable; and it must end.

In the information technology world we are on the verge of dramatic new breakthroughs in data-mining capabilities that are giving ordinary analysts an extraordinary ability not just to search but to analyze and to understand enormous quantities of data from a vast array of different data sources. The cutting edge of intelligence analysis, in other words, is likely to be in so-called crunching massive amounts of data on a genuinely all-source basis, drawing upon multiple data streams in ways never before possible, but possible today.

However, as long as we have no one, Mr. Chairman, in a position to see all the many data streams that exist within the Federal Government, much less those that may also exist in the State and local arena and in the thriving information economy of the private sector, all of these rapidly advancing data-mining analytical tools will be of little use to us.

Already, Mr. Chairman, it has been one of our frustrations on this committee to see the degree to which even agencies that acknowledge the importance of interagency electronic information sharing are each independently, yes, independently, pursuing separate answers to this problem. We heard a little of it today.

Even their responses to the problem of agency-specific stovepipes are too often themselves stovepiped responses. The DCI's own initiative to create an Intelligence Community-wide Intelligence Community system for information-sharing depends wholly upon agencies deciding what information they think other agencies' analysts need to know. Every agency will be charged with populating its own shared space that will be searchable by clear and accredited on-line users. No outsider, it seems, would ever have access to an agency's real databases.

This is exactly the type of thinking that I think we must—we must purge from our Intelligence Community. We need new ideas and a genuine appreciation in the Community's top management of information technology and how it can be exploited to attack the target.

Mr. Chairman, as we saw last week, the most innovative ideas put forth by our witnesses were more money and more people—yes, more money and more people. Unless we see some new thinking and leadership within the Intelligence Community, Mr. Chairman, I believe that more money and more people will get us, yes, more of the same. That we do not need.

Mr. Chairman, I would like to submit for the record an article by Stan Hawthorne entitled "Knowledge Related to a Purpose: Data-Mining to Detect Terrorism." This article, I believe, effectively discusses the need to integrate our information systems. I commend it to my colleagues. I have a copy here for the record.

Chairman GRAHAM. The document will be entered in the record.

Vice Chairman SHELBY. Mr. Andre, in your remarks earlier you suggested that there might be problems with information-sharing in part because of overly restrictive interpretations by Intelligence Community lawyers of the existing law and executive orders. Do you think progress in information-sharing has been impeded by the development of a mythology of restrictions that encourages day-to-day, hour-to-hour decisionmakers to assume more barriers exist than actually do exist?

Mr. ANDRE. Yes, sir, I do. That was the point I was making. There is nothing wrong with the laws, but the interpretations have unduly constrained us in receiving some information.

Vice Chairman SHELBY. You have seen examples of that, have you not?

Mr. ANDRE. Yes, sir.

Vice Chairman SHELBY. How can we on this committee and Members of the Senate and the House, how can we dispel any such myths and focus on what the law actually provides? Is that a question of education of the people involved in the various agencies?

Mr. ANDRE. Yes, sir, I believe it is. The word "culture" was mentioned a number of times, and I think it is very understandable over the past couple of decades how we have gotten so afraid to touch certain categories of information. As was mentioned, there were penalties for crossing that line.

I think we have an initiative within the Department of Defense to go out and educate the inspector generals, the general counsels and the intelligence oversight people as to what the law really says and how in today's threat environment it might be interpreted.

Vice Chairman SHELBY. You were not here last week, but you may have followed the hearing. But there was a lot of confusion about the criteria for FISA, and even some of the witnesses—I believe Chairman Graham asked some questions on this and others, too, that maybe some of the FBI lawyers didn't really understand the criteria for FISA that they were dealing with every day. We were astounded here. But I bet you have seen that in the Community yourself, have you not?

Mr. ANDRE. In spades, yes, sir; and it has trickled down to every level. The analysts have been conditioned not to ask for certain kinds of information. We are changing that, and they are getting more aggressive.

Vice Chairman SHELBY. They should ask for anything that has probative value to what they are doing.

Mr. ANDRE. Yes, sir. When they are being told no, we are pushing it up and pushing it up the Hill. What we have to do is mount an aggressive assault on all sources of information, and that is exactly what we are attempting to do.

Vice Chairman SHELBY. How do we do all-source information, that is, bringing all relevant information regarding a possible terrorist strike or anything from every quarter to a single collective source? Is that correct?

Mr. ANDRE. Yes, sir.

Vice Chairman SHELBY. That is easier said than done, but it has to be done, doesn't it?

Mr. ANDRE. Yes, sir, because the understandings of the laws, the interpretations of the laws, creates seams that the bad guys understand and they take advantage of. I am convinced of that.

Vice Chairman SHELBY. But as long as you have all these separate kingdoms or whatever you want to call them, you will never have a fusion of information consistently at the right time and the right place, will you?

Mr. ANDRE. No, sir.

Vice Chairman SHELBY. Mr. Andre, Acting Director Jacoby—and this was touched on earlier today, but I just want to be clear—said in his statement for the record that we need a paradigm shift in the ownership of information within the Intelligence Community. Those are strong words, but they have meaning. Rather than allowing the agency who collected information to control which analysts are permitted to see this information, Admiral Jacoby suggested, as I understand, that we need to ensure that ownership of information resides with analysts.

Is this DIA's official position, or would you like to elaborate on that?

Mr. ANDRE. I don't know that it needs much elaboration.

Vice Chairman SHELBY. It speaks for itself, doesn't it?

Mr. ANDRE. Yes, sir, it does.

Vice Chairman SHELBY. What steps do we need to take here in the Congress to create a system which analysts are empowered to access any, any information they need in order to do their job? Because that is the key, isn't it? All bits of information coming together in a collective mode makes the whole, doesn't it?

Mr. ANDRE. Yes, sir.

Vice Chairman SHELBY. You have some suggestions?

Mr. ANDRE. If I were king, which I am not, I am not even a minor warlord, I would——

Vice Chairman SHELBY. Let's make you the crown prince, for the sake of conversation.

Mr. ANDRE. What I would start with is information standards. That is the starting point. In order to start managing our information collectively, we have got to put the information into a form that it can be managed. We are not there today.

We believe in DIA that that standard is, as was mentioned earlier, Extensible Markup Language, XML. We don't have to achieve systems interoperability, which would cost a lot of money and cause a lot of pain, but if we have data interoperability, even if the data were to reside in separate repositories——

Vice Chairman SHELBY. Go over that again. I think this is a very important point. You are not just talking to the committee here, you are probably talking to the world, at least the American people. Explain what you are talking about again.

Mr. ANDRE. Yes, sir. Much like occurs in the commercial sector, we would not have to own or control or maintain a single data repository that has all the data. If the data were appropriately configured, empowered and content-tagged, that is, not tagged at a record level, security classification and authorship, but the meaning of what is in that, the data, law enforcement data, for example, could be in one pot, sensitive compartmented information could be in a second pot, unclassified data could be in a third pot.

We are really talking about a giant server farm. We have the analytic discovery technologies, the relational tools and the mining technology to search across those data repositories as long as the data are compatible.

I think, and I am not an expert, I am not an IT person, but I have been told we can resolve many of the security concerns and concerns with things like discovery by keeping them segregated, but when one needs—when one is working a threat issue or an offensive option issue, that they can search across all of those data repositories and continue to not only find linkages in the data but begin mapping that knowledge by tagging it at the analytic level for the benefit of the next person that accesses that little piece of data. That is knowledge mapping.

Vice Chairman SHELBY. Where they don't start all over.

Mr. ANDRE. They don't. We start that during the collective expertise of any analysts who scrutinized that data and left his or her fingerprint on it.

Vice Chairman SHELBY. All-source ought to mean all-source, shouldn't it?

Mr. ANDRE. Yes, sir. I think I was pretty emphatic about putting the "all" back into all-source data.

Vice Chairman SHELBY. Commissioner Norris, first of all, I want to thank you for being here today. Your oral and written statements were disturbing to me and, I suspect, to my colleagues.

Is it your assessment that the Federal Government is the impediment to information sharing among local, State and Federal agencies; and, if so, why is this the case?

Mr. NORRIS. Well, it is my assertion. We rely on them almost completely for analysis data we uncover, information to help us

protect our cities. And, again, we don't need the sources and method, we just need to know what the threat is for operational reasons.

But I think what has been said here before, it is not certainly the people at the street level. They do their job no matter what. It is not as much an IT problem from my perspective. It is what has been spoken about a couple times before. It is a cultural problem. It is this culture of secrecy, I guess, in withholding information; and I think people hide behind the fact that, a lot more than they should, that they can't disclose information. Things are classified too often that need not be. Most information can be unclassified.

Vice Chairman SHELBY. If they can't disclose some stuff, they can't help you.

Mr. NORRIS. It is very hard to declassify something. You know how long that takes and what a process it is. But something that shouldn't be classified in the first place should be. A lot of the information should be out there for our consumption. These are just some of the problems we are encountering.

We are not unlike a lot of other American cities. The problem we are encountering now is getting people vocal about it. I don't know why people are being, frankly, so quiet and polite about it. I mean no disrespect when I say we are not getting the help. We just want to speak the truth and get some relief in our cities, our urban populated areas.

Unfortunately, while many of my colleagues will complain privately very loud they are not getting anything, they have no idea, and when confronted or asked how is everything going, they smile and say things are great.

There are a couple of vocal police chiefs around the United States who have been sticking their neck out, and, frankly, there is a handful that have been saying this publicly. I can assure you it is privately held by many more.

Vice Chairman SHELBY. We appreciate your candor.

In the past year, how many times have you asked the FBI to brief you on Baltimore-area terrorism investigations? Roughly?

Mr. NORRIS. Oh, a couple of times. We just never got the briefing in the first place.

Vice Chairman SHELBY. Has the FBI ever provided that briefing?

Mr. NORRIS. No, not yet. My question is, I would like to know exactly what is being worked on in my city.

Vice Chairman SHELBY. Sure. You believe that this same situation that you have in Baltimore is being repeated in other cities throughout the country?

Mr. NORRIS. I know that.

Vice Chairman SHELBY. Sure. Is this a basic cultural problem with the Bureau?

Mr. NORRIS. That is a question you may have to ask the other side, but that is my feeling, it is, yes. I see no reason why that chiefs of major American cities—I know we have this discussion here in Washington with Chief Ramsey and others and in Philadelphia. We have people working on task forces. There are detectives working on joint terrorism task forces that can't even tell us what they are working on, and they work for us. If you can't trust your police chiefs in your major cities, maybe they shouldn't be there. If

that is the case, you know, we have a big problem here. We need to know what is going on in our jurisdictions.

Vice Chairman SHELBY. We need to solve the problem of working together.

Mr. Greene, we understand that, prior to September 11, that the CIA refused to provide the names of suspected terrorists at INS unless the Agency believed that these terrorists were actually coming to the United States. Only then would the CIA bother to put names into the State Department-INS computer bases that are designed to look out for suspected terrorists. After September 11, we understand the CIA changed its policy and gave the State Department and INS a great many names of suspected terrorists that it had refused to share for a long time. How many new names appeared in the INS database just after September 11 when the CIA stopped withholding information like that?

Mr. GREENE. Mr. Shelby, I can tell you that over the last year the number of names that have been entered into the TIPOFF System are a little over 14,000.

Vice Chairman SHELBY. Fourteen thousand.

Mr. GREENE. A majority of those are terrorism-related, although some of the TIPOFF stuff relates to Russian organized crime.

Vice Chairman SHELBY. Before September 11, this was not given?

Mr. GREENE. That is correct, sir.

Vice Chairman SHELBY. The joint inquiry staff has identified, Mr. Greene, over 1,000—yes, 1,000—CIA documents containing terrorist names that were not provided the State Department and INS databases before September 11. I am asking you the obvious question; do you believe these names should have been shared?

Mr. GREENE. Yes, sir, I do.

Vice Chairman SHELBY. If the names of the two hijackers from San Diego had been in your database earlier, would your agents possibly have been able to stop them upon their arrival at a U.S. port of entry?

Mr. GREENE. We think there is a likelihood that could have happened, yes, sir.

Vice Chairman SHELBY. But you didn't have those names, correct?

Mr. GREENE. No.

Vice Chairman SHELBY. They were not given to you. This information was not shared?

Mr. GREENE. That is correct.

Vice Chairman SHELBY. Governor Gilmore, what are the appropriate limits, if any, upon the nature and extent of intelligence information that should be shared with State and local government officials involved in counterterrorism work? In other words, what is the best way to structure such information-sharing? You have been the governor of a big State.

Mr. GILMORE. Senator Shelby, the philosophy that the Commission has taken in advising the Congress is the key importance of a partnership between the Federal, States and locals, because they are all doing different kinds of activities. Information is largely gained from international sources only at the Federal level, but a lot of information is gained into the overall system from police

chiefs, fire departments, State police, narcotics investigators, people all over the United States that reach far beyond any place the Federal Government can possibly go because of the limitations of resources.

So once the concept is adopted that it is a total partnership in order to create a national strategy, then the question is what type of information do you ask for and how should that go.

The answer is I think you can give the information to give reasonable information and warning.

Mr. ANDRE. Analytical ability to people at the States and local areas, and they can give information back again as well.

There are safeguards that apply today to Federal intelligence organizations that could easily be applied vertically up and down the line. I think the information that the States and localities want is what is the nature of warnings and threats information that has been obtained, how legitimate is it, how does it impact on the activities of people at the State and local level. That then allows the States and locals to become more of a partner in the overall protection of the people of the United States.

Vice Chairman SHELBY. Mr. Chairman, my time is up. Thank you.

Chairman GRAHAM. Thank you very much, Senator.

We now are at the point where individual members will be given five minutes for questions. I am the first of those. Then Congresswoman Pelosi, although she might yield. Then Congressman Roemer and Congressman Boehlert will question, in that order.

I am very interested in the issue of terrorists among us. To me, of all of the links of the chain that threaten the people of the United States, one of the most, if not the most, significant is the fact that a particular nation or organization has a capacity inside the United States of trained and placed operatives who are willing and capable of conducting terrorist assaults against us, as we saw so dramatically on September 11 of last year.

In a closed session it was stated that one of the targets to try to disrupt and avoid the enlargement of those operatives inside the United States would be a closer scrutiny on those persons who we had reason to believe had gone through a training camp and then were trying to return to the United States or enter the United States for the first time. We are getting a significant amount of data from the results of the war in Afghanistan on that subject. Now the question is, how can we apply it?

This question is particularly to Mr. Greene and to Ambassador Taylor.

We issue visas from most of the countries that are of greatest concern to us to applicants within that country for entry into the United States. How much utility have the intelligence agencies made of your visa lists to match it against lists of suspect persons to determine if there are people already in the United States or to be on the watch for persons who might be attempting to enter the United States?

Mr. GREENE. I will start from the interior, Mr. Chairman. As I mentioned to you earlier, the information that we are currently getting from the various agencies of the national Intelligence Community and the 14,000 number that I mentioned to Mr. Shelby ear-

lier includes but is not limited to CIA cables, but that is giving us a capability when we expand the use of IBIS to people who are already within the United States, for example, applying for benefits, to use that intelligence in a way that we have not been able to before.

One of the other things that I mentioned, which is the special registration program under the NSEERS system, is allowing us to focus not only on five countries that have been identified by the Attorney General as needing to participate in this special registration process but also allows for the individual inspectors within certain guidelines and based on certain intelligence to require other people from other countries to register as well.

So I think that there is a greater expansion of the information that we now have access to in terms of who poses a potential threat to the United States, in addition to identified targets by name as a result of intelligence work overseas.

The challenge for use is—as we said to Congressman Hoekstra, seven million illegal people in the United States by estimates. The challenge is for us to devise a risk-management strategy that would allow us really to focus the resources that we have in the interior on identifying those people who pose the greatest potential threat. It is based on the intelligence that we receive from the various components in the national Intelligence Community that in part helps us devise a system that allows us to manage that risk effectively.

Chairman GRAHAM. I would like to ask a quick question before turning to Ambassador Taylor. Could you assess in a few words where are we in terms of implementing the system that you have just outlined?

Mr. GREENE. We are just starting.

Chairman GRAHAM. Ambassador Taylor?

Ambassador TAYLOR. Yes, sir. As I mentioned in my opening remarks, Mr. Chairman, we have received from the Intelligence Community a large amount of data that has gone into the TIPOFF and eventually into our lookout system that we continue to evaluate in terms of people who have been issued visas, as well as people through the INS that have come to the United States.

So the great influx of that information has been very useful in making the TIPOFF and CLASS database available for the entire community as a source for information on potential violators or others that we need to go find or indeed not let back into the country, not let into the country.

Chairman GRAHAM. To exercise the Chairman's prerogative for one quick follow-up question, what percentage of those persons on your TIPOFF list are also in the database for the interior activities? Is it 100 percent?

Ambassador TAYLOR. It is available completely to the INS.

Chairman GRAHAM. When it is my next turn, I am going to be asking some questions of Governor Gilmore and Commissioner Norris, to stay on the theme of the terrorists among us.

Nancy, do you want to defer?

Ms. PELOSI. I defer.

Chairman GRAHAM. Congressman Roemer.

Mr. ROEMER. Thank you, Mr. Chairman.

I want to thank our excellent panel again for a very helpful analysis and very compelling testimony today. We have talented people from elective office, from the different agencies around Washington, D.C.

I want to especially commend you, Commissioner Norris, for your very honest portrayal, blunt portrayal of where you think this system is or where it is not.

Let me ask you a couple quick questions, and I only have five minutes, so if you can be brief, as you have been, I will sure appreciate it.

When we move in this elaborate color code system that we have developed here in Washington, D.C., to try to warn our local communities, whether Baltimore or South Bend, Indiana, my hometown, and we go from a Yellow Code to an Orange Code, which is the second highest code of alert in the country, what happened to you as the commissioner of one of our larger middle-sized cities when that code was changed? Did you get phone calls? Did you get alerts? What happened?

Mr. NORRIS. Of course. Actually, we didn't. We got phone calls from the elected officials in the city and public, but we didn't get much information, or any, from the Federal Government as to why, which is again our issue, when it goes up.

It also costs the—the Federal Government, when they raise the level of alert, it costs municipalities a great deal of money if they respond in kind, because it requires us in many cases to go to 12-hour shifts, protect certain locations, do a whole lot of things you would not be doing in your ordinary, routine patrol.

Mr. ROEMER. Did you kick in all those things that cost your local government more money?

Mr. NORRIS. We did. Because what we found—in that case I described, that was the same day. We found that, simultaneously with the elevation of alert, we found that group of eight men with the suspicious documents and the like. So we did kick it up for a couple of days.

Mr. ROEMER. But what you are kind of saying between the lines, if I am reading it correctly—you correct me if I am not right here—is if you don't get a phone call from the Federal Government or from the FBI or somebody, you just simply see it only TV, and that happens over and over, you are probably not going to incur the costs of 12-hour shifts and other things if that kind of trend continues?

Mr. NORRIS. That is true. We don't know. The threat, is it the same in Los Angeles as it is in New York and Baltimore and Miami? We need a little more information—we need a lot more information than that, frankly. You are correct. That is right.

Mr. ROEMER. So this is pretty frustrating for you, the color code system we have right now?

Mr. NORRIS. Right now, yes.

Mr. ROEMER. You need more information and more direct contact with the Federal Government and more information-sharing, more collaboration?

Mr. NORRIS. We need to be day-to-day partners in this, is what we need to be.

Mr. ROEMER. Right. Let me ask, we have a very talented person from the CIA here, Mr. Pease, who was sworn in when we had the witnesses stand. Let me ask, if I could, Mr. Chairman, to Mr. Pease, if he were to receive information, very credible information about an impending attack on the City of Baltimore, what is the process by which you would alert Mr. Norris about this direct threat to his city, Commissioner Norris?

Mr. PEASE. Mr. Roemer, if it is something that specific, a threat to Baltimore, almost regardless of the type to Baltimore, you would expect immediate phone calls to be made to their security apparatus. Our normal first point of contact would be the JTTF if it is intelligence-based information. Most likely ours would be. The JTTF is the FBI-led interagency task force that is designed to pull together information on terrorist threats.

Mr. ROEMER. You call them. They are located where?

Mr. PEASE. There is a JTTF in Baltimore. There are 50 some nationwide.

Mr. ROEMER. Mr. Norris has been saying the communications between the FBI, the 60 agents there, and his police force is not good.

Mr. PEASE. I am suggesting an apparatus already set up to get instant classified information from us to Baltimore electronically would be through the JTTF. You could also guarantee that phones would be picked up. Our Deputy Director of Central Intelligence for Homeland Security, a new position with Mr. Winston Wiley, has already been in contact with the Commissioner, and I would expect that person-to-person contact would be made very quickly.

Rarely do we get information that is so narrowly cast as a particular city.

Mr. ROEMER. How would you assess then whether or not you pick up the phone to do that? How narrow does it need to be to engage in that kind of process?

Mr. PEASE. There is an attitude to get threat information out as soon as possible, and it permeates through our apparatus. I know the Director of Central Intelligence would be picking up the phone. They have that type of attitude. The mechanism that exists is via the JTTF, but we also have thinking human beings that are inclined to pick up a phone. We know that we need an established mechanism that has not yet been invented for reaching out to all the apparatus of homeland security in a way that makes that apparatus feel both comfortable and well served.

Mr. ROEMER. My time expired. I thank the Chairman.

Chairman GRAHAM. Thank you, Mr. Congressman.

We have next Congressman Castle.

Mr. CASTLE. Thank you, Mr. Chairman.

I toured homeland security offices, and one of the things that was explained to me there is something that Commissioner Norris and perhaps others touched on today, and that is the need to work with the local communities and how important that is and how they are the ones that can identify the trouble spots or perhaps even the cells or whatever it may be. I think that is a very accurate statement. It is something that is going to take a long time to implement correctly.

But I also have watched in the Intelligence Committee as we have these very Top Secret briefings, and I pick up major news-

papers the next day and read about 90 percent of what was told to us. That is not leaking. That is just information that generally did not have to be classified as Top Secret or whatever it may be.

We have had some discussion here of all-source analysts and even the open source materials or whatever it may be. But then we also had some discussion by one of you of the length of time it takes to get somebody cleared so they can get the information which is necessary to do your job, whatever it may be.

I am becoming increasingly concerned about this. I think there is a reaction in the Intelligence Community, and I can understand it and I don't mean to be harassing, because I believe there are intelligence matters that should be kept Top Secret, there is no question about it, but I think there is an easy out, and that is to overclassify it by stamping Top Secret on virtually everything that goes through an office in order to make sure that nobody is ever accused of letting something go that shouldn't go. As a result of that, I think we are having problems sharing the information that needs to be shared with a lot of the agencies represented here today.

We worry about the communications between CIA and FBI, and those are things we have to work out. But I am concerned about the classification circumstances and the inability of all of your various agencies to understand what the problems are.

INS, for example, needs to see who is on a list of people who should not be coming into the United States of America. If for some reason or another that isn't cleared fast enough to get to them, that is a problem.

I don't have the answer to this. I don't have precise defined knowledge on exactly what the problem is. But, as I talk to experts, they usually come to the same conclusion that we need to do something about it.

I am interested in any brief comments any of you may have about that particular subject. I know it is a general subject. I don't expect you all to have the answers. I don't know, Governor Gilmore, or anybody else, if you actually looked into it in the work you are doing, but I would be interested in your comments on that.

Mr. GILMORE. Congressman, are you asking what would facilitate information-sharing?

Mr. CASTLE. I am asking essentially if you agree that there is a lack of information—any of you, in the various agencies you run—going to you. Is part of the cause of this the issue of classification of intelligence at too high a level so you don't get information which really could be made more public, if you will, which would help you in your job, plus it stymies you in terms of bureaucracy to get that done? That is what I am asking. Anybody can answer that.

Mr. GILMORE. I will make one brief analytical comment, and I think the agencies themselves would have a more practical response. But, you know, what kind of setup do we presently have? What kind of culture does it exist within? It is, if you get sensitive information, you get it from a sensitive source, then all of the pressures are against disclosure. You might make a mistake. You might disclose something to someone who doesn't have a need to know. There is no system in place to make that kind of decision.

So the tendency I think is to err on the side of caution and not give information, as opposed to a culture that would say, no, actually we need to get this information into the hands of the police commissioner in Baltimore.

Mr. CASTLE. That is correct. If that is the case, should the Intelligence Community be cutting this more sharply than they are now? Would that help in terms of the information which is needed out there?

Mr. GILMORE. There just needs to be a different attitude about getting information out to the right people. Governors, for example, don't get this information. I don't recall getting any intelligence during the four years I was governor of information on any kind of threat whatsoever. I suppose there was some low-level information from time to time to our State police and things like that. In terms of high-level threats against the Commonwealth, it wasn't there. There is no setup for it to be there.

Mr. CASTLE. They are making them more set up now that we have the homeland security, and we are dealing with the local police agencies more.

Any other comments?

Mr. NORRIS. I agree with you, because one of the things that has been frustrating for us is, as in the case I disclosed before, I talked about we worked on the same person, but the explanation was certain things they can't tell us because we weren't cleared. And while that may be true, that shouldn't be the case, because, number one, it is incredibly dangerous to both work on the same people with undercovers throughout the city. Second of all, that just should not be the case. It is either an excuse or, if it is a fact, it needs to be an obstacle that is overcome.

Frankly, just to touch on Congressman Roemer's question and address yours, when the threat is specific, you don't even need a clearance in many cases. Because we got something once when anthrax was—right at the time it was very hot last year, there was a direct threat to Baltimore. It came from overseas. The FBI called me immediately. In a specific threat case like that, I didn't need to know the source or methods. I didn't need a clearance. They just told me, there is a threat, 1:15 today, you are going to be attacked from anthrax. It came from I can't tell you where. But with that little bit of information, we were able to protect ourselves. That is what we need, frankly.

You know, you are absolutely right. You can either declassify them and don't stamp them at the highest level, or speed up the clearances of people that need them, if that is the case.

Mr. GREENE. Just a quick comment. From the INS perspective, the issue you raised, Congressman, is very dear in terms of the kind of action we can take with respect to people who are on lookouts. If the name is in the lookout system because it is based on classified information and that person is taken into the INS administrative law system and processed for deportation, then in order for us to do anything other than handle it as a routine immigration case, which would allow them to be entitled to bail, allow them to be able to leave the country voluntarily and all of those benefits that attend to that, it is dependent on declassifying the material upon which the lookout is based and being able to use that in this

administrative law forum. Of course, that is very difficult, especially if there is—depending on the sources and methods used.

So we find ourselves frequently caught in a dilemma where we have someone who we suspect does pose a threat to the United States and yet, because of the level of classification and of the unwillingness to declassify that in a manner that allows us to use it in the public administrative forum, we have to treat it like every other administrative case.

I think what happened in Baltimore recently is an example of that.

Mr. CASTLE. I can't see the lights, which is wonderful. I assume my time is up. I didn't know that for sure.

I would like to say, Mr. Chairman, in closing, if we are going to deal with 700,000 local police or law enforcement officials, it just seems to me we need to look at the whole broader system of what we are doing with intelligence in this country if we expect that to help. I hope it is something we as a group will look at.

Chairman GRAHAM. Thank you, Congressman Castle.

Congresswoman Pelosi and then Congressman Boehlert.

Ms. PELOSI. Thank you very much, Mr. Chairman.

Gentleman, welcome. Thank you for your service to our country.

A special welcome to the police chief of Baltimore, a city near and dear to my heart. My father and brother always said in politics and in keeping people safe, always look after—my father would say the men in blue, my brother would say the men and women in blue, a generation later. Thank you for your service.

Your presence here today points out how much our work on homeland security has to be about localities, localities, localities. We say location, location, location are the three most important words in real estate. But localities, localities, localities are the most important in protecting our people. So the testimony you are giving to us is valuable, and I hope this inquiry has one purpose, but I hope in what Congress does in the bigger picture in terms of homeland security we will take heed of what you are saying about having access to the information and improving the communication.

I was interested, also, Governor Gilmore, in your testimony about your Commission and its valuable work in which you have said what really made your panel special and therefore causes its pronouncement to carry significantly more weight is the contribution from members of the panel from outside of Washington, D.C., that you brought in fresh eyes on the subject and innovative thinking. Although you had some participation from the establishment, you had fresh eyes. That is what those of us who have been advocating an independent commission for September 11 have been advocating as well. Congressman Roemer has been the leader on that issue, and your testimony is useful in that regard.

I wanted to use the first five minutes of my time to talk to Mr. Manno about the President's Commission on Aviation Security and Terrorism of years ago. Was it 1989? 1990? May, 1990. In that Commission on Aviation Security and Terrorism, the report makes some pretty stark comments. It says the Commission's inquiry finds that the U.S. civil aviation security system is seriously flawed and has failed to provide the proper level of protection for the traveling public. This system needs major reform.

It further goes on to say the Commission has conducted a thorough examination of certain civil aviation security requirements, policies and procedures surrounding Flight 103. This is Pan Am. That is that particular flight. It is a disturbing story that goes on to tell how that all happened.

It recommends an Under Secretary for Intelligence at the Department of Transportation, at the FAA. Is that the job you hold, Acting Secretary?

Mr. MANNO. It is the Office of Intelligence and Security that works directly for the Secretary of Transportation. It is DOT as opposed to TSA, that I work for.

Ms. PELOSI. You work for TSA. We have FAA, we have TSA now, and we have the Department of Transportation. There is some relationship there.

Mr. MANNO. Yes.

Ms. PELOSI. There is a different job established by this Commission.

Mr. MANNO. Yes. That office was established to provide support and advice directly to the Secretary on issues of transportation security, not just aviation but transportation security. That office was, in fact, set up.

Ms. PELOSI. Okay. Now in the report one of the recommendations says the FAA and the Federal Bureau of Investigation should proceed with plans to conduct an assessment of the security threat at domestic airports. It is my understanding that these assessments are made on an annual basis.

Mr. MANNO. I think they are made on a three-year basis. There are a series of them that were done. The latest iteration, there were some that were done, the latest in 1999, and then some more airports were done in the year 2000. So it is an ongoing process.

Ms. PELOSI. Is it your understanding that any of those assessments ever pointed to use of airplanes as weapons as a possible threat to our domestic security?

Mr. MANNO. Not to my knowledge.

Ms. PELOSI. So these assessments would have missed that.

Mr. MANNO. What those assessments do in terms of the threat information that the FBI provides is that they look at the threat environment around the airport that they are looking at in terms of terrorist activity, criminal activity in order to be able to provide the airport, mainly, an idea of the environment that they are operating in, so that they can then have or develop contingency plans to deal with that.

Ms. PELOSI. Since I don't have much time, I appreciate that. But it must have reported about the possible threat of hijacking, for example.

Mr. MANNO. I believe what they report on is the presence of terrorist groups and the kinds of activities that they are maybe involved in in that local area.

Ms. PELOSI. That might be hijacking but not use of airplanes as weapons?

Mr. MANNO. It could be. I am simply not aware of any at that point.

Ms. PELOSI. There is one place where the Commission called for a recommendation to assess the danger, the risk, where informa-

tion was possibly missed in these assessments that were being made about the threat.

Mr. MANNO. I don't know if there was any information that actually pointed to such.

Ms. PELOSI. Tell me what your job is. You are the Under Secretary for Intelligence at——

Mr. MANNO. I am the Acting Associate Under Secretary for Intelligence at TSA. When TSA took over aviation security and security for the other modes, we are now responsible for assessing the threat to aviation.

Ms. PELOSI. My time has expired, would like to close by saying that I appreciate all the good intentions, and I know that if you read this book you will weep because it predicts, it tells you what we should have done as far as aviation security is concerned. And it is from 1990, the President's Commission under senior President Bush. And it calls for, I think, a more comprehensive—as excellent as the work that Ms. Hill and the joint inquiry staff has done, it really speaks to the fact that while we have come down hard in terms of our analysis of what was going on in our country and the role of the FBI and CIA, there are other agencies that had a responsibility to protect the American people. We must assess their performance as well, and we must do it with fresh eyes if we are truly going to live up to our responsibilities to protect the American people from terrorism.

My time has expired, but I look forward to the next round.

Chairman GRAHAM. Thank you, Congresswoman Pelosi. The next questioner will be Congressman Boehlert, followed by Senator Feinstein, and then Congressman Gibbons.

Mr. BOEHLERT. Thank you Mr. Chairman. I have a rather general question for all the panelists, and why don't I pose it first, and then I will get to Mr. Greene with a very specific question. But this is the most diverse panel we have had in the hours and hours and hours of hearings we have had and therefore one of the most valuable.

It has been my observation that we have spent an inordinate amount of time listening to those in the front lines in the Intelligence Community—and we can understand that, the FBI and the CIA—and constantly we hear from them that the problem is resources, people, and flexibility. They say that after talking about all the success stories they've had—and there have been many and we should all be thankful and appreciative of that.

You know success has many parents; failure is an orphan. But we don't hear about the success stories. And dedicated men and women in the Intelligence Community are on the front lines every single day, and because of that so many attempts have been thwarted. We just never hear about them. But the failure we hear about repeatedly, day after day, hour after hour. And it is a failure that we're addressing and we're trying to get to it.

I would suggest we're never going to have enough resources. We're never going to have enough people. And we're never going to have Lucy-Goosey laws and rules, so anything goes. But I would suggest that the problem is more of communication, coordination, and interpretation. And you are all reinforcing my thinking in a way, so I thank you for that.

And I want you all to ponder this, and I will start first with Governor Gilmore. If you were to give us one bit of advice on the one thing that you think we should focus on, if you were to change chairs with me and give me the advice to follow through in these hearings, what would that one piece of advice be? And ponder that, and I will get specifically to Mr. Greene.

We have learned during our previous hearings that Zacarias Moussaoui was an illegal alien. He was out of status as of May 22. And, being out of status, he enrolled in aviation school, and he did a lot of things that were very visible and very public and no one caught him. And then on the 15th of August of 2001, the FBI launched an investigation and discovered he was out of status, and did nothing for awhile.

And my immediate response is, why didn't you throw him right in jail immediately because he was out of status? And the response is, well, we are going to pursue this because we think we might learn something from it.

There is a big national debate going on about a national ID card, and you know what that debate is all about. But I would suggest there has to be some sort of document or card that serves the purpose for all people who visit the United States, with biometrics and everything else, all the technology we have at hand, so that we could immediately track someone who is out of status the moment they are out of status. Would you comment on that, please?

Mr. GREENE. Yes, I'd be happy to. It is frankly with that particular mission in mind that we have looked at both the NSEERS system and the SEVIS system that I mentioned at the beginning of the hearing. SEVIS is a system that allows us to track students and exchange visitors who are coming into our educational and training institutions. It allows us to determine whether they've reported to those institutions in conformance with their visa and whether they maintain their status as students or trainees under the conditions that the visa allows. It's a system that is already generating information for my special agents to go out and start looking for.

So we already are significantly far ahead of where we were a year and a half ago with respect to being able to identify students who fail to maintain the conditions of the visa.

Mr. BOEHLERT. What was Mr. Moussaoui's status when he was legal?

Mr. GREENE. I don't know, sir. I'll have to check. I believe he was a nonimmigrant visitor.

Mr. BOEHLERT. Are we just going to check the students?

Mr. GREENE. The NSEERS system is the larger system that allows us to handle all nonimmigrants. Obviously it is a much larger universe of people.

Mr. BOEHLERT. Do you have a specific timetable for implementing this?

Mr. GREENE. We do have a particular phased process that we are working out.

Mr. BOEHLERT. I hope it's not going to be like some of the Presidential Commission reports that we read that says we ought to do something about it and then gathers dust and we go on to something else.

Mr. GREENE. Well, you're dealing with a universe potentially as big as half a billion people a year. So it's complicated in terms——

Mr. BOEHLERT. It is, but the technology is there. I am privileged to chair the Science Committee, and I know a little bit about technology. It's there. We've got the means, if we've got the will and the wallet.

My red light is not on yet. Let me ask you each of you—Governor, I would like you to start. If you were to change places with me, what would you focus on as a member of this very important panel—and I think it is doing outstanding work and in large measure because of the very excellent, capable, hardworking, and dedicated staff; what would you focus on?

Mr. GILMORE. Congressman, this committee has focused a great deal of attention on the ability to share information back and forth among Federal agencies and continues to do that. And it's very much a focus even of this meeting here today. The focus has to be, in addition to that, how you get information up and down the line between Federal, State and local. That is something that is not being widely discussed and mechanisms are not there to do that. Clearances are not there, and above all things, the culture is not there.

Mr. BOEHLERT. So, for example, you would suggest that when the Director of Central Intelligence on December 4, 1998 declares war on al-Qa'ida, it would be nice if other people in the Intelligence Community knew about that declaration of war and were similarly engaged.

Mr. GILMORE. It would be just as important for people in Los Angeles, New York, Virginia, Montana, and California to know about that and the facts connected with it as well.

And the second thing I would say, Congressman, is I think we should all keep an eye on civil liberties and make sure we don't fix things so well that we begin to impinge upon the civil liberties of the foundation of the country.

Mr. BOEHLERT. Let me tell you that nobody up here wants to rip up the Constitution and throw it away. Chief, what would you advise me and what would you pursue?

Mr. NORRIS. If we were really going to be radical about this and pursue things, I would look toward creating a system much more like they have in England, where you have a domestic intelligence agency and an operational agency. As long as we have law enforcement agencies competing with each other, no matter how you try to change the culture and tell people to get along, if we are all in the business of locking up terrorists, bad guys, criminals in general, it doesn't work.

One of the reasons we get along with some of the other agencies much better and share information is because intelligence agencies are not in that business. And I would look with an eye toward doing that, creating a domestic intelligence agency and an operational law enforcement agency just to pursue terrorists.

Mr. BOEHLERT. Mr. Greene—the red light is on, but they're answering my question.

Chairman GRAHAM. This is going to be the final question.

Mr. BOEHLERT. Final answer.

Mr. GREENE. The particular challenge that I face is bridging that gap between intelligence and enforcement information. Intelligence information can cover a variety of types of data about the particular people we are interested in. To make that jump from intelligence into information that I can use in a public forum to deport somebody is very critical. And that gets to the risk-management sort of thinking that I suggested earlier. I think that's a real challenge for all of us to look at.

Mr. BOEHLERT. Thank you for your indulgence, Mr. Chairman.

Chairman GRAHAM. Senator Feinstein.

Senator FEINSTEIN. Mr. Chairman, I would like to enter into the record the transcript of a hearing that we held in the Judiciary Committee, the Subcommittee on Technology, Terrorism and Government Information, on October 12, 2001.

Chairman GRAHAM. Without objection.

[The document referred to, entitled The Role of Technology in Preventing the Entry of Terrorists into the United States, a hearing before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary, U.S. Senate, October 12, 2001, Serial No. J–107–43, is voluminous and is retained in the files of the Joint Inquiry Committee.]

Senator FEINSTEIN. Thank you very much. And I want to read a brief part of that hearing transcript. We had before us Mrs. Mary Ryan, Ambassador Mary Ryan, Assistant Secretary for Consular Affairs at the State Department, and I was asking her the question essentially: Why did 16 of the terrorists receive visas?

And this is the answer. "What went wrong is we had no information on them whatsoever from law enforcement or from intelligence. And so they came in and applied for visas. They were interviewed and their stories were believed. I think like most Americans, I was surprised at how much we learned about some of these terrorists in the immediate aftermath of the September 11 atrocities, and the question in my own mind is why we didn't know that before September 11.

"We were asked by the FBI to revoke visas on August 23 of 2001. And we found that one person they had asked us to revoke we had no record of. Another had been refused. A third one, his visa had expired, and the fourth one obviously we revoked, but he was already in the United States.

"We have had to struggle with the law enforcement and Intelligence Communities in getting information. We have tried in the Bureau of Consular Affairs my whole time in Consular Affairs to get access to the NCIC III information from the FBI and we were constantly told we were not a law enforcement agency and so they couldn't give it to us. Other agencies fear compromise of sources and methods."

And there's much more in this along that line. But more than a year ago, the USA PATRIOT Act was passed. And one section of that Act sought to address two concerns by directing the Attorney General and the Director of Central Intelligence to establish training programs for State and local officials which would, one, allow them to effectively identify foreign intelligence they may come upon and get it to the right people; and two, to be effective consumers of intelligence.

My question is for the non-Federal members of the panel, beginning with the distinguished Commissioner. The law establishing these programs has now been more than a year old. Has anyone either from the Department of Justice or the Intelligence Community approached your agencies offering training? Have there been any concrete results that you have seen of this initiative?

Mr. NORRIS. I guess the short answer is no. No one has briefed us on training or offered it, and frankly we haven't seen much of a difference since this has been passed.

Senator FEINSTEIN. Anybody else, non-Federal agency?

Mr. GILMORE. Senator, I want to make a general observation. In our Commission report, third report, we make reference to some survey results and the purpose of our survey which was to over 1,000 State and local agencies across the United States. We asked questions about Federal programs, whether they were aware of them, were they effective, were they efficient, and we have produced that data into our reports to make it available to the Congress. And the answer is, generally speaking, it's mixed. Sometimes people know about the programs, participate in them, and find them effective. Very frequently they do not.

Senator FEINSTEIN. Also pursuant to the Enhanced Border Security and Visa Entry Reform Act, which is also now passed for a substantial period of time, the Act required the following: that the INS fully integrate all data systems and databases maintained by the Service and that the fully integrated system be a component of an intraoperable data system to be used by all relevant Federal agencies in detecting and deterring the entry of foreign terrorists.

Mr. Greene, what steps has the INS taken to upgrade and integrate the Agency's technology systems to comply with the new Federal requirements under the Border Security Act?

Mr. GREENE. I know there is a project under way to meet the requirements of that Act. I am not current as to the status of that project, but I would be happy to brief you or your staff when we get that information.

Senator FEINSTEIN. Can you give us any estimate of how far along you are?

Mr. GREENE. I am just not aware of that particular area, so I will get back to you as soon as I can.

Senator FEINSTEIN. Are you aware of any of the obstacles to ensuring that all INS officers at the ports of entry and district personnel in Interior, any obstacles to them having the right hardware, software, and sufficient training?

Mr. GREENE. My understanding of the problem is that INS information systems, as you know, grew like mushrooms according to need over the last 20 years. So we have distinct systems to deal with distinct program mission requirements. Putting that together is a software problem, and that's what the project is about.

Meanwhile, in terms of the integrated lookout system, IBIS, which I mentioned to you earlier, that's now accessible to all inspectors at ports of entry as well as to all of our officers and the Interior officers. And NAILS is being used at the LESC as a screening process. But in terms of being able to integrate every single system, that's a long-term project and I'm just not—I don't want to go too far down the road giving you information about it

without making sure that I know what I am talking about. So let me get back to you on that.

Chairman GRAHAM. Thank you, Senator. Congressman Gibbons.

Mr. GIBBONS. Thank you, Mr. Chairman. Gentlemen, welcome. It's a pleasure to have you before us today.

What I would like to do is relate to you a conversation that I had and have had many times with some of our local policemen, whether they are Capitol policemen or policemen back in my home State. It's regarding the issue de jour, the issue that we're here about; that's information-sharing.

The story relates to an incident in which the policeman came upon a car—and this just happened to be one here in Washington, D.C.—in which there were four individuals, Middle Eastern background, one had an expired driver's license. He was not driving. The other three individuals in the car had no identification. They were pulled over for a minor traffic violation, stopped, questioned.

His comment to me was he's prohibited from checking the legality of their status in the INS. And therefore they were released because there was no way for him to find out any information about these individuals. It was a minor traffic violation. He did not know whether he had in his hand the next four individuals who may be conducting a terrorist attack.

So, Mr. Greene, let me ask you what legalities, what barriers, and what regulatory obstructions are there that prevent local police, first responders, from getting to necessary information to be able to ferret out from this 500 million individuals those people that are here not legally in a timely fashion that could make a difference before the next terrorist attack?

Mr. GREENE. As I mentioned earlier, the Law Enforcement Support Center which has been in operation for more than ten years is designed specifically to address that particular area. In terms of somebody that is already in custody in local police, that can be done without any additional keystrokes. It is a matter of when you do the NCIC check, you also check out an IAQ screen and it automatically queries INS databases and gives you that information.

Mr. GIBBONS. I understand that and I think everybody here understands that we have a database that has known terrorists in it, a database that has known individuals with wants and warrants in it that can be checked.

Mr. GREENE. The Support Center goes beyond that, sir. It really has access to every single data system that the INS has.

Mr. GIBBONS. That goes back to Senator Feinstein's question.

Mr. GREENE. That's correct. We have people 24/7 that can go into the different systems that INS has and do a comprehensive check.

Mr. GIBBONS. How long does that take?

Mr. GREENE. The average is about seven minutes back to a police officer who is on the phone. That's the national average. They do approximately 15,000 queries a month from local law enforcement for that particular purpose. And those special agents who are located at the LESC can in fact put a detainer on somebody who is being arrested by the local law enforcement officials.

Mr. GIBBONS. They still have to know that the individual is a known terrorist to be able to be in that system.

Mr. GREENE. They can actually identify in that system people who are simply immigration violators or wanted absconders.

Mr. GIBBONS. Let me turn to Commissioner Norris and ask that question of you. Do you feel that your line policemen and -women on the street can access INS data without feeling restricted, impeded, or in any way prevented from having full use of that data when they do a routine traffic stop?

Mr. NORRIS. That's the key. We have had great cooperation, especially post 9/11, with the people from INS but it requires a phone call. That means we have people in custody for other reasons. From the scenario you gave before of people being stopped in a traffic stop, it's not likely—no one would have a phone.

What happens in our business, unfortunately it is always 2:00 in the morning on a Saturday night when we run into these folks. And the way it's done in the police world is via a hand-held radio. And if the names were in NCIC that's how we would get them. We wouldn't have access to that database from the street unless they are already in custody. But they have put—my understanding they have put wants and warrants into NCIC so if someone is wanted we have access to it. But as far as this, they would already have to be in custody for us to access it.

Mr. GIBBONS. So there is no legal, constitutional, or regulatory barriers that prevent anyone who is making a normal routine inquiry into a traffic violation or something of that minor sort to query INS with regard to the legal status of an immigrant?

Mr. GREENE. Can I address that, sir? I am not a lawyer but any police officer can voluntarily and consensually request anything about anybody, but the question is what do you do with that. And recently the Department of Justice indicated that there is no Federal prohibition for a law enforcement officer in making an inquiry or even effecting an arrest of a civil immigration violation. It is the State provisions of the State constitution and the opinions of the State attorney generals that might pose an obstacle. But the Federal system itself does not.

Mr. GIBBONS. Mr. Chairman, I will wait for another round to continue this questioning.

Chairman GRAHAM. Thank you, Congressman Gibbons. We have now completed the first round of questions. We are going to start a second round. During my questioning I said I wanted to focus on the issue of the terrorists among us.

Commissioner, what do you know about the status of terrorists—and I am going to define a terrorist as a person who was recruited and trained specifically for the purpose of having the skills of conducting terrorist operations and then was placed into your community to await a call for action. Do you have any sense of how large or if there is such a community of persons in Baltimore?

Mr. NORRIS. No, sir. We have not had that—I have actually asked that question of other chiefs. When they say, "Oh, no, I get all the information," I said, "Really? How many people do you have in your city like this?" And that's the question I pose to them.

The answer is no, I do not. And it's just the people we unearth as we go through our routine police duties like the ones I described before. That's what gives me pause. If we're finding this, what's really out there in our cities that we don't know?

Chairman GRAHAM. If you were going to write your description of what you would like to know about these individuals in order to be of greatest value to you in your law enforcement responsibilities, what would you like to know about that community in Baltimore?

Mr. NORRIS. I would like to know exactly what everyone else knows in my city. Whatever Federal agencies are working on in my city or any other city, I should know exactly what's happening. The people you're describing, people that had been recruited, we know for a fact the terrorists are living in our cities. We all know they're here; we just don't know who they are, we being the urban police departments in this country.

I would like to know and I would like to have a briefing, if not every two weeks, at least every month. I would like to know what's happening, because I get briefings from my intelligence division every day, so I know who we're working on and I know what we're looking at—information we come across. If I had access in a full briefing from whatever agency investigating within my city, it would make my life a whole lot more efficient and comfortable. I would like to know what is happening, but currently do not.

Chairman GRAHAM. Governor Gilmore, I am going to ask you to step back into your previous life as Governor of the Commonwealth, where I assume you had the title of the chief law enforcement officer of the State. Was that the responsibility of the Governor in Virginia?

Mr. GILMORE. Certainly; and together with the Attorney General, of course.

Chairman GRAHAM. To ask the same question that I just asked the Commissioner, did you know when you were Governor as to the existence of terrorists—individuals, or in cells—and what would you have liked to have known about them?

Mr. GILMORE. Well, the answer—short answer is very little, if any. The State police may have had some of that kind of information that they accumulated from their own investigations and their own observations in working together with local law enforcement people as well. But I don't believe there is any established pattern of communication between Federal intelligence organizations and any State officials.

We approached it differently. We simply went to work on it to begin to prepare the systems that would go into place in the event of an attack, prepared to notify the State police to go on alert to warn about hostages or any type of gunplay, communication with naval authorities and military authorities, the ability to activate the National Guard. We put into planning steps that would be taken in the event of such an attack. And sadly enough, they were implemented on September 11.

Chairman GRAHAM. So would you say that, because in large part your lack of information, you were forced into the position of being reactive to an event that already occurred as opposed to being proactive to avoid that incident?

Mr. GILMORE. Absolutely. In this instance, of course, it was an attack on the Pentagon. And I don't know whether information supplied to Virginia could have prevented an attack, but it could have been something else and we don't have any system set up. We

are simply prepared for what incident might have happened. And on that day, we moved forward from a standing stop.

Chairman GRAHAM. When it's my next round of questions, I am going to ask some of the representatives of the Federal agencies who are here to answer the question of what are the barriers to providing the information that the Commissioner and the former Governor indicated they would like to have and what would be your evaluation of the public policy implications of overcoming those barriers; that is, are there any national security boundaries that we should be aware of and, if so, how would we describe those boundaries in terms of information that should not be made available to State and local law enforcement?

Congressman Goss.

Chairman GOSS. Thank you, Mr. Chairman.

I think, Mr. Andre, you said terrorism is criminal. I certainly agree with you. It's also intelligence. And it's also integration and it's local law enforcement and it's a whole bunch of other things, too. And it's obvious from what we're hearing today that other committees of jurisdiction in the United States Congress are going to want to exercise their oversight in areas that go beyond the intelligence portfolio. Our purpose here is to link up the intelligence product that the capabilities of our Nation, which our taxpayers invest in to provide us the product for our wellbeing, is getting to the people who need it to do their jobs to make sure that wellbeing actually happens.

And we are identifying breakdowns today. Part of our problem is, frankly, we are focused on terrorism but we don't know exactly what terrorism involves. It's a broad definition and it keeps moving. Nevertheless, overcoming that, I think we understand it when we see it and we're trying to deal with it.

So, Mr. Manno, I want to go to a direct question following on another Member's question to you: Are we profiling now at airports for national security purposes for safety in our airline traffic?

Mr. MANNO. We have a passenger prescreening process which is based on what we have learned about how terrorists operate that we in fact use to identify those people for additional scrutiny. That's in addition to the specific information, the watch lists.

Chairman GOSS. What you're basically saying is that there are behavior patterns of people who come in that there's no preinformation on that you're screening.

Mr. MANNO. Travel patterns.

Chairman GOSS. So that is a behavioral pattern rather than any ethnic pattern or any characteristics, physical characteristics.

Mr. MANNO. That's correct. It's not based on race or ethnicity or anything else. It's on the behavior that we have seen and studied.

Chairman GOSS. Let me just ask you a couple of questions. I haven't been aware that there's a serious problem with youngsters or some of my more experienced senior citizens involving hijacking airliners, and yet they are caught in the screening process. Makes me think that there is a random process in place for screening which we get a lot of commentary about actually, and I am sure you do too, and not filling people with confidence at this point. And on the other hand, you get the other side of that argument as well,

that we are profiling and that is an intrusion of civil liberties. So tell me about the random searches.

Mr. MANNO. There is a certain percentage of randomness and what that's designed to do, again because we know the opposition studies everything that we do. And we don't want—we want to do whatever we can to not enable them to figure out patterns, you know, the methods that we are using. So there is a small percentage, actually very small.

Chairman GOSS. Basically we should be telling the American people is, look, we have a procedure at the airports and we are not going to tell you what it is because the enemy is listening and we just ask you to bear with us. Is that where we are?

Mr. MANNO. We definitely don't want the enemy to know.

Chairman GOSS. I am not making judgment, I am just trying to understand it because we have these questions in our offices.

Mr. MANNO. And the answer, yes, there is a passenger prescreening process that we are using and that has a certain level of randomness in it.

Chairman GOSS. If I am terrorist, I should take note we have a system in place and we're going to catch you.

Mr. MANNO. We are going to try our best.

Chairman GOSS. If I am an American citizen I shouldn't ask right now, because we want to have a safe flight. I don't find anything unreasonable about that as long as we are a little bit more candid with the American people, because trying to tell them that searching some of these folks who have trouble getting on the airlines unassisted and thinking that they are going to hijack the plane does defy credibility.

Mr. MANNO. Just one additional comment, if I may. The system I just talked about was something that actually had been in place a number of years. We are in the process of coming up with another system that is going to be refined that tries to address some of the things that you mentioned that is a better system. And you know we are working towards that——

Chairman GOSS. I am not trying to be critical. I am trying to share with you the kind of observations we're getting from the public.

And, Mr. Greene, the question I'd have for you is, do you have adequate enforcement capability? Because our experience with all of the good things your Agency tries to do shows us that enforcement is an important part of it, and there doesn't seem to be enough. Is that an accurate observation?

Mr. GREENE. That is an accurate observation.

Chairman GOSS. Could you give me a hint of the degree of the problem?

Mr. GREENE. We have less than 2,000 agents who I can field to do street investigations on any given day. Approximately 400 of those are in special dedicated projects like OSIDEF or JTTF or antismuggling agents working for Border Patrol chiefs. On any given day, without leave, I can probably field 1,300 agents in the field for an emergency; seven million illegal aliens in the United States—the math speaks for itself.

Chairman GOSS. Thank you, Mr. Chairman. I hope the terrorists weren't listening to that answer.

Chairman GRAHAM. Senator Shelby.

Vice Chairman SHELBY. Thank you, Mr. Chairman.

President Bush, back in May when he signed the Enhanced Border Security and Visa Entry Reform Act, he said: "We must know who's coming into our country and why they're coming. It's knowledge necessary to make our homeland more secure."

Now today, October 1, we don't really know—in other words, you don't know who's present even in this country today, everybody that's come in here, legally, illegally, legally overstayed. Is that a correct statement?

Mr. GREENE. That's correct, sir.

Vice Chairman SHELBY. And basically at this point you don't have the system in place to track people, know exactly where they are, when they come into the country legally and they overstay their visa, and how you are going to pick them up and get them out of here or whatever?

Mr. GREENE. That's correct. We have a system that provides us with some limited capability in that regard, but we're working toward the goal.

Vice Chairman SHELBY. And you need help. I understand. You need resources. But having said all this, some of you are probably familiar with, a couple of weeks ago, Mr. Brent Scowcroft, who is very well respected in the security business. General Scowcroft, he sat right here at this table; in his judgment, the safest place in the world for terrorists was in the United States of America. That's frightening. I hope that's not true, but I kind of believe it might be true. So we have our challenge, do we not?

Mr. GREENE. Yes, sir, we certainly do.

Vice Chairman SHELBY. Mr. Andre, you spoke eloquently this morning about the potential for cross-database, data-mining and information-sharing. You spoke a great deal about the community, how the community should approach these problems. Why aren't we hearing this from the DCI? How much of what you described is actually being implemented at the Intelligence Community level currently as of today?

Mr. ANDRE. I don't think I'm in a position to answer that.

Vice Chairman SHELBY. You don't know, do you?

Mr. ANDRE. No, sir, I don't know.

Vice Chairman SHELBY. Governor Gilmore, you spoke about the need for a government-wide all-source fusion center for terrorist threat information. Do you think that a new Department of Homeland Security, which we keep debating, would be a logical place for such an organization?

Mr. GILMORE. Could be, Senator. The sense of the Commission is it may be more effective as a stand-alone agency, one similar to EPA or a structure of that nature, reporting directly to the President for supervision purposes. But that is the sense of the Commission, as opposed to placing it within one department.

Vice Chairman SHELBY. But if you had a stand-alone agency, how would it function? If you report to the President, couldn't you be creating another bureaucracy?

Mr. GILMORE. Well, you could. It would be the danger. The sense of things, though, is that there is—and the Commission thought about this—we tend to be very reluctant to recommend to the Con-

gress or to the President the establishment of yet another piece of bureaucracy. We tend to approach things with great reluctance. The challenge we were looking at is where else can you put this in order to make it effective as a fusion center for CIA, FBI, NSA, State police departments, local police departments, FBI. Where does it reposit in order to achieve that? And the thought was that an independent stand-alone agency might end up being the best possible option.

Vice Chairman SHELBY. Mr. Pease, could you come up to the table and I'll ask you the same question. Why aren't we hearing from the DCI regarding the database, cross-database, data-mining and information-sharing? You know, we haven't yet. Will we hear from them and when?

Mr. PEASE. I think you'll certainly hear more on 10 October when he's scheduled to testify next in the open. We have talked about both the existing mechanisms that are working better lately, like to the CT Link that helps us share classified information and the need for more of those.

Vice Chairman SHELBY. My time is up, Mr. Chairman.

Chairman GRAHAM. Thank you, Senator Shelby.

Next will be Congresswoman Pelosi, and then in order, Congressmen Roemer, Gibbons, Boehlert.

Ms. PELOSI. Thank you, Mr. Chairman.

Mr. Andre, first I wish to extend condolences of my constituents, and from my colleagues, to the families who lost their loved ones in the Pentagon, working bravely for the DIA to protect our country, and welcome you in that spirit.

My question was about force protection which, of course, up until September 11 was our main focus in terms of intelligence to protect our forces. And some of those forces are in the United States. If, for example—well, we can use Baltimore as an example. Are there any bases still left in Baltimore?

Well, we'll go to California then. We have some there. If you had intelligence that a base in San Diego was threatened, do you have a way—or do you have a way to channel information to the local police on that so you can let them know? And if they get the intelligence first, do you have a well-established channel of communication from that direction to the DIA?

Mr. ANDRE. Actually, we do. One of the elements that's embedded in the Joint Intelligence Task Force for Counterterrorism are the security and investigative arms of the military service; for example, NCIS agents and Air Force OSI agents that have domestic law enforcement authorities and are quite connected to and wired into their colleagues assigned to security details or bases around the United States. So that's a very active and very reliable channel both for two-way flow. It is that bridge for us between the law enforcement and foreign intelligence world for domestic threats.

Secondly, you might have seen an article in today's Los Angeles Times announcing an experiment that we are conducting with CADIC in California and with the New York Police Department and the new Northern Command and Defense Intelligence Agency using what is called RiskNet. It's an unclassified law enforcement network to share information. It's only at the unclassified or for official-use-only level, but we think it offers some real potential be-

cause we may not, to use Admiral Jacoby's paradigm, we may not own a lot of information we can share but there's no constraint on us loaning our brainpower, our analytical expertise to local authorities.

Ms. PELOSI. I assume everything you said applies to the Office of Naval Intelligence as well in terms of your communication.

Mr. ANDRE. Yes, ma'am. They are embedded.

Ms. PELOSI. Thank you.

Mr. Pease, is the CIA prepared to share the kind of background data to all sources across the Intelligence Community required to do the analysis without filtering the information?

Mr. PEASE. Indeed we have made some conscious choices, especially since 9/11, to put more and more of the raw information out as published intelligence, so that there's very much less that is on what anybody would call the "cutting room floor." There will always be a certain filtering when you get to the identity of the source and the circumstances of meeting that source. And analysts across the community have said we do not want that information—or do not want that information. The problem for us has been, and remains, the repository that has that information and also has other information. It is simply a challenge to pull the information that they do not need, and we don't want to give up, and let them see the rest of that database.

Ms. PELOSI. Following up on that, Governor Gilmore, can the Homeland Security Department Intelligence Directorate, which has been proposed, function without access to raw data and/or function as the fusion center referred to earlier? And you elaborated on wanting it to be separate. So why don't we focus on the raw data side of it?

Mr. GILMORE. No, I think they would have to have raw data in order to be able to apply proper analytical skills to that, depending upon what the nature of the division would be, whether it is going to receive information already through analysis and then determine how they want to use that information, or whether they want to go through an analytical process themselves.

Ms. PELOSI. If I may, Governor, do you think that that entity should be able to task for getting additional follow-up intelligence on information they have received?

Mr. GILMORE. Yes, Congresswoman, and we have recommended that to the Congress.

Chairman GRAHAM. Thank you, Congresswoman Pelosi. Congressman Roemer.

Mr. ROEMER. Thank you again, Mr. Chairman.

Mr. Manno, the alleged terrorist Ahmed Ressam was stopped on the way to the Los Angeles airport in January 2000. The FAA did some analysis of his bomb equipment. What did you find with regard to that bomb equipment, and did it relate to other terrorist trends or activities?

Mr. MANNO. I think what our bomb techs found when they looked at it was that there were some similarities in the timer that Ressam was in possession of and some of the timers that were used by Ramzi Yousef.

Mr. ROEMER. So what you found at that—when did you do the analysis? He was stopped in January, January 2000. When did the FAA make that tie to Yousef?

Mr. MANNO. What our bomb techs did, and I don't know the exact date, but they worked with the FBI Bomb Data Center to come to that conclusion. They were not identical.

Mr. ROEMER. But you made some conclusions that it was very similar to Yousef, who had helped devise the plot in the Philippines in 1995 to blow up airliners across the Pacific Ocean.

Mr. MANNO. Yes. However, the other components that he was carrying in the vehicle kind of indicated that what possibly he might have been going after was a different type of target, possibly using a car bomb, because there was a large amount of explosives as opposed to the smaller, more sophisticated devices that Yousef had been working on.

Mr. ROEMER. I just want to see how you reacted to this. If you could get for the committee how long it took you to put this together and when you did associate some of the similarities between the timer that Yousef and the timer that Ahmed Ressam was going to use? Did you then disseminate this information to other law enforcement agencies or did you have discussions with other groups outside the FAA?

Mr. MANNO. We had internal discussions with the people that look at countermeasures. The way we did security in the FAA at the time was, we would assess the threat, collect all the information, and then provide it to the operations and policy people within the Agency, who then looked at our existing measures to try to determine whether or not the baseline measures we had in place would be able to counter the particular threat that had just been identified or whether additional measures would have to be applied.

Mr. ROEMER. So you had these internal discussions, but the intelligence agencies had been brought into this plot, the Bojinko plot in 1995. Why wouldn't you expand this outside the external conversations within the FAA and go back to the intelligence agencies or the FBI and share this information, which I would think would be significant, that this timer is very similar to something being used in a plot that involved a host of different airliners and had two or three key people associated with it with the Bojinko plot.

Mr. MANNO. Our bomb techs did work with the FBI.

Mr. ROEMER. How about the CIA and intelligence people who had shared the information with the—I guess it was the Philippines initially, according to public documents.

Mr. MANNO. I don't know if the FBI went back to the CIA with that. I don't believe that we did in a formal way.

Mr. ROEMER. Why wouldn't you though? Why wouldn't you be looking at all the different sources at this point to try to discover if you have a similarity to extend this through law enforcement channels and intelligence agencies to really get at the root of this?

Mr. MANNO. Well, again, our focus at the time was, because of the similarity that we had identified, was to try to determine if this was some sort of a plot against aviation. The indications weren't there, other than the similarities of the timer. Yousef had gone through training in Afghanistan along with many, many others and

this was a common technique that was taught in the camps. So that part itself was not unusual. There was no other information that we were aware of that would tie Ressam at that time to a plot against aviation. It wasn't until much later.

Mr. ROEMER. I think I am running out of time, if I haven't already. I would just say whether it was tied to a plot, you are tying him to people. The equipment may be tied to people in the Philippines with similar intentions. And I would have hoped that that would have been followed up on.

Chairman GRAHAM. Thank you, Congressman Roemer, and we will have a third round if you would like to continue to pursue that.

Congressman Gibbons and Congressman Boehlert.

Mr. GIBBONS. Let me take off on just a little bit different approach to this intelligence-sharing question which got going here today. There are two opportunities for the United States Government to interface with an individual who is attempting to either visit or immigrate to the United States, the first being of course our consular offices that are overseas and our embassy where this individual will approach to get a visa. And the second is our port of entry, Customs or whatever.

Let me ask—and I don't know if this is a question for State Department, and I don't see the Ambassador here, but if anybody could answer—are all our consular offices overseas equipped with the same systems, same databases and the same capability as each other would be? Is it a uniform system that is available? And obviously there is going to be an individual speaker.

Mr. KOJM. I am going to invite Tony Edson from the Bureau of Consular Affairs, who took the oath as I did at the start of the hearing and ask him to respond to the question.

Mr. EDSON. In the aftermath of the first World Trade Center bombing, we were given authority to retain visa fees, and used those funds for a major systems development and deployment exercise.

Mr. GIBBONS. So we're talking in 1993.

Mr. EDSON. Beginning in 1994.

Mr. GIBBONS. What's the current status today?

Mr. EDSON. As of 1998 the platform was uniform worldwide, and it remains that way today.

Mr. GIBBONS. Who provides consular offices or the INS with the information necessary to make a judgment and the evaluation of the acceptability of a visa applicant?

Mr. EDSON. If I understand the question correctly, it's a combination of factors that come into play there, of which the lookout information that's available to us through the CLASS system that's been discussed today is one of those factors. It's the primary factor for antiterrorism information.

Mr. GIBBONS. So all consular offices have access to the data and can make a judgment as to what's in these database systems on every applicant for a visa?

Mr. EDSON. Yes. It is physically impossible to enter data on an individual applicant into our system without generating the check against these databases as a background task.

Mr. GIBBONS. Including fingerprints.

Mr. EDSON. Not fingerprints, except on the Mexican border.

Mr. GIBBONS. Mexico City is the only consular office that does a fingerprint check or fingerprint documentation.

Mr. EDSON. And Mexico City and our border posts along the Mexican border.

Mr. GIBBONS. Let me go to the INS. What information is available on these individuals to our border guards that are standing security on our borders? How do they know when somebody presents them with a document that it isn't false, that they are the right person, and this person is not a terrorist on one of our watch lists, whether it is NAILS or any other system?

Mr. GREENE. There are a couple of things that have happened that have improved that. One now is our access to the consular database that allows us to pull up a picture and a copy of the nonimmigrant visa application as it was executed overseas at the time the visa was issued.

Mr. GIBBONS. That is current on every border crossing?

Mr. GREENE. That is current on every border crossing, every port of entry. We also now are incorporating the IDENT system, which is the two-print identification system, into the IBIS system. We are expanding that usage. So certainly, as was indicated by my State Department colleagues, along the southern border we can do that identification now at ports of entry as well as between ports of entry, and that is expanding to the northern border.

Mr. GIBBONS. Going back to the consular question, let me ask you a question. Local law enforcement agencies have information about individuals that may go to, A, their reattempt to get a visa if they've left the country. Is that information inputted into the INS system? If so, how is it inputted? And how long does it take for that information to get there?

Mr. EDSON. This actually might be a question better addressed by my INS colleagues.

Mr. GREENE. Our NAILS system, which is the primary lookout system for the INS, is input primarily by field agents—either deportation officers, inspectors, or special agents—based upon information that they get from local jurisdictions with respect to convictions and facts that might disqualify them from being able to enter the United States again. So that system goes in and I believe it is refreshed up into IBIS within 72 hours.

Mr. GIBBONS. Thank you, Mr. Chairman.

Chairman GRAHAM. Congressman Boehlert.

Mr. BOEHLERT. Thank you, Mr. Chairman.

Mr. Greene, how many nonimmigrant aliens are there in the United States today?

Mr. GREENE. I don't know, sir. I know that it could be as high as a quarter of a billion that come in annually. I mentioned earlier, it's half a billion transactions every year at our ports of entry; that is, airports, seaports and land border ports. And if you cut out the commuters and the returning citizens and so forth, it comes down to about a quarter of a billion. The nonimmigrants could be half of that.

We may in fact be able to give you numbers of the number of nonimmigrants who are admitted on a yearly basis, but that would be historical data. I don't know what it is today at this moment.

Mr. GIBBONS. The answer is we don't know.

Mr. GREENE. That's correct.

Mr. BOEHLERT. What is the estimate of that 250 million nonimmigrant aliens in the United States that are out of status?

Mr. GREENE. Again I don't think we know that. We don't know the answer. The information that we have, the systems that we have relied upon over the last 20 years, are simply inadequate to give us an accurate picture.

Mr. BOEHLERT. Wouldn't you think this would be rather important information to have?

Mr. GREENE. It is, absolutely, and it is information we're attempting to address by establishing this NSEERS process which will give us an effective biometrically-driven entry/exit system that will allow us to determine who has come into the United States and who has left.

Mr. BOEHLERT. Which leads me to the NSEERS program. On page 4 of your testimony you say, under NSEERS, INS is fingerprinting and photographing nonimmigrant aliens who may potentially pose a national security risk upon their arrival in the United States. "Who may potentially pose," is that a judgment call or is this all nonimmigrant aliens?

Mr. GREENE. It's not all nonimmigrant aliens at this point. NSEERS is being implemented on a phased basis. So what we started at some port of entries and what is fully implemented today—as of today at all of our ports of entry is the simple registration process under the NSEERS system. That involves nationals of five countries who the Attorney General has designated are either state sponsors of terrorism or require special registration as a result of this. It actually builds on a system that has been in place for a number of different countries for more than four years. It is the first of a system or of a set of steps that will allow us to fully implement an NSEERS system for all nonimmigrants, but the special registration part deals strictly at this point with nonimmigrants about whom the United States has a special concern.

Mr. BOEHLERT. You're striving toward 100 percent.

Mr. GREENE. That's correct.

Mr. BOEHLERT. And what's the anticipated date to achieve that 100 percent?

Mr. GREENE. I am not sure it's settled yet. It's an interplay between how quickly we can do it and how much it will cost.

Mr. BOEHLERT. You don't have an idea—two years, five years, ten years?

Mr. GREENE. I don't have an idea, sir.

Mr. BOEHLERT. Wouldn't that be a good idea to have that idea?

Mr. GREENE. Yes, it would.

Mr. BOEHLERT. Could you provide the committee in a timely fashion some specifics to my line of questions?

Mr. GREENE. I'd be happy to.

Mr. BOEHLERT. Under what we already have in place, it's a small fraction of a percent of what we hope to achieve. I am just trying to think—none of the hijackers, the 19, would have been caught up in this NSEERS system? Maybe one or two of them.

Mr. GREENE. It's unclear because, in addition to the five countries, there is also a series of discretionary registrations that might

have caught some of them, but it would be speculative to say. We have roughly——

Mr. BOEHLERT. We have roughly 250 million nonimmigrant aliens in the country and we don't know how many of them are out of status.

Two things. I think we should know the answers to those questions. There doesn't seem to be a bell that rings anyplace or some sort of mechanism that's triggered that would indicate someone is out of status. We don't have the foggiest idea if some of these nonimmigrant aliens are still here or someplace else. I think what we are learning is we know what we don't know, and what we don't know is a hell of a lot.

Mr. GREENE. I think that's right. Systems were not designed to provide a foolproof way of tracking nonimmigrants who came into the United States. And remember that according to INS estimates, only 50 percent of the people who are considered to be illegal residents in this country come from nonimmigrant visas. I mean the threat, as you know, from—has always been conceived of unrestricted immigration along the southern border.

Mr. BOEHLERT. I am well aware of that.

Mr. GREENE. That has been pretty much where the focus has been for a long time, and it was really the events of the attacks that prompted us to look in a very concentrated way about how do we improve the systems that can track and monitor the people who are coming in here with legal visas.

Mr. BOEHLERT. But we think we have something to improve it, but we don't have any idea how much it is going to cost or when it is going to be implemented. I don't mean to be sort of argumentative.

Mr. GREENE. No, sir, and I don't mean to leave you the impression we don't know. I know what I don't know, and I know the discussions are going on now about how to adjust pacing to finance to the amount of money. We will just give you a full briefing on that when I get back and find out what that is.

Mr. BOEHLERT. I can't expect you to know everything. It would be comforting to me if you had a better idea on this particular one.

Mr. GREENE. And I apologize to you on that.

Mr. BOEHLERT. No apologies are in order. We are all on the same team trying for the same thing. We are trying to develop foolproof systems across-the-board. I just want to be helpful.

Mr. GREENE. We can give you a very thorough briefing on that.

Mr. BOEHLERT. Thank you so much.

Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Congressman Boehlert.

We will now start a third round. I would like to use the history of Khalid al-Mihdhar to probe a few of my questions. Al-Mihdhar was one of the participants in that January 2000 summit of al-Qa'ida that was held in Malaysia. He then entered into the United States two or three weeks thereafter, and after a brief stay in Los Angeles, moved to San Diego. He was in San Diego by February of 2000.

To follow up on Congresswoman Pelosi's question about what would we do if we had someone who had suspect background in terms of being a terrorist who happened to be in a community with

a major U.S. military facility, well, we now have that situation, someone who we surveilled at a summit of terrorists who is now in a community with major U.S. military interests.

Was whoever was responsible for security of places like the San Diego Naval Air Station and whoever would be responsible for civilian law enforcement in the San Diego area, were they notified of the presence of a person who was a very highly suspect for terrorist activities individual? Do you know, Mr. Pease?

Mr. PEASE. If you are talking about August of 2001——

Chairman GRAHAM. In February of 2000, when they arrived in San Diego.

Mr. PEASE. In February of 2000, absolutely not.

Chairman GRAHAM. Why would neither the Department of Defense officials or a local government official have been notified of the presence in their community of someone who just a few weeks earlier had been a participant in a summit of terrorists?

Mr. PEASE. You are asking basically the same question as why do we not have a watch list at the time. I think we covered that in
separate decision made to share it with some rather than others.

We do have our record traffic that says that the visa information, the multiple entry visa information, was passed to the FBI in January of 2001, but that was the extent of our sharing at that time on that particular incident.

Chairman GRAHAM. That was ten months after.

Mr. PEASE. Excuse me, I said 2001. I meant January of 2000. But that was the extent of our sharing at the time on this particular case.

Chairman GRAHAM. Assuming that someone was alert to the characteristics that I have just described, known not only as just a garden variety terrorist, but someone who was high enough up to be invited to this high level meeting in Malaysia who is now in a major U.S. city which happens to also be a very significant defense establishment, if someone were focused on that set of facts and alert, what would they be expected to have done?

Mr. PEASE. I can tell you that under today's standards, we would indeed put out a published intelligence report on Mihdhar's travel and the meeting in Malaysia that indeed would have gone to both Department of Defense and the regional command, in this case Pacific Command, that would have been responsible for the local security of a naval facility in San Diego.

Chairman GRAHAM. Would it have gone to the civilian law enforcement agency?

Mr. PEASE. Indeed, it would have gone to FBI and several other departments.

Chairman GRAHAM. Including Commissioner Norris' counterpart in San Diego?

Mr. PEASE. From our own practices, for that type of information, especially when we would not know whether Mihdhar—where Mihdhar was entering into the United States, it would be up to the FBI to decide which amongst the local police departments would be getting further information. That has been their call. That system is subject to change, but it has not changed.

Chairman GRAHAM. I want to ask one more question about Mihdhar. Mihdhar left the United States in the fall of 2000 and in June of 2001 he was in Jidda, Saudi Arabia, where he applied for either a new or renewal of the passport which he had had which had lapsed some time previously.

On his visa application, he was asked this question: Whether he had ever been in the United States. He checked "no." Now, he not only had been in the United States, but he had come through the Los Angeles airport with a valid U.S. passport at that time.

What was the gap in the system that did not pick up the fact that he had just committed perjury by falsely answering the question as to whether he had ever been in the United States, when we must have had some documentation that he had been in the United States, because he had come through our immigration system.

Mr. EDSON. When he applied, we would routinely have searched his old passport for travel patterns. But when he applied for this visa, based now on the automated record, we can only assume he didn't submit the previous passport which would have shown that entry into the United States, so we had nothing in any of our systems to record the entry into the U.S., the departure from the U.S., that would have shown he was on the application.

Chairman GRAHAM. Excuse me for taking another question. Did the people in Jidda have access to the information that this man had previously held a U.S. passport?

Mr. EDSON. Yes, they would have known he had a previous U.S. visa.

Chairman GRAHAM. Is it standard procedure when a person is applying for a new visa or a new passport, the previous one having expired, to ask to see the previous passport?

Mr. EDSON. Sure. If it comes to the attention of the interviewing officer, it would have been standard. It was about three years prior to this reapplication.

Chairman GRAHAM. Is that a standard question that is asked, have you ever had a U.S. passport?

Mr. EDSON. Have you ever had a previous U.S. visa? It is on the application form.

Chairman GRAHAM. But would it have been possible within our data system to have confirmed the correctness of the answer to that question?

Mr. EDSON. Yes.

Chairman GRAHAM. But you assume it wasn't checked in this case?

Mr. EDSON. Right. I would assume it wasn't checked in this case.

Chairman GRAHAM. Congressman Goss.

Chairman GOSS. Thank you, Mr. Chairman. In the area of breaking news, I have just been informed that there is a 10-year-old who is having a birthday tonight who is maybe a starting pitcher on a local baseball team whose mother happens to be sitting about three feet behind me. I think it would be very important that we wish Brian Hill a happy birthday and make sure his mother is there at the opening of the game. So my questions will be short. The first pitch is at 6:00, which is good news for our panel.

The last series of questions that I wanted to get to was we have had a lot of testimony today about frustration, as a nation of laws and who we are, that sometimes we haven't been able to get the things done that we might have wanted to get done to protect ourselves better and we have perhaps erred a little bit on the side of caution, being a free democratic society that cherishes our civil rights. That is not all bad news. The question is, what improvements can we make if we need to?

Now, if I have got it right in my notes, I believe Mr. Andre said that the laws were not the problem, the policies were the problem, and I think Mr. Greene suggested that we did have some problems with some of the laws, and I suspect that the answer is both, that we do have problems with both.

Then we have had in previous panels a lot of discussion about—in the Intelligence Community we call it risk aversion, and in the law enforcement community we call it don't rock the boat. In various iterations, as we have gone through our discussions, it has come down to sort of a culture of it is not necessary to go too far down this road, because it is probably a bigger threat to cause a fuss or have a bad photo op, it is going to cause my career more trouble or whatever the case may be, so why don't we just not do it.

Then there are probably very justifiable reasons. What I would like you to tell me is, is that something that we legislate or try and legislate in this country, or is that something that we just try and keep reflecting the will of the people we represent across the board as it changes?

I am very much seized with the impossibility of trying to draw a line somewhere that says we know where the line in the sand is, exactly here, where national security protection comes exactly up against your freedom to do what you want and your civil rights as an American citizen or visitor in our country. I don't know where that line is exactly. I don't believe we have had any testimony that calls for any specific legislation, but if there is, we would like to know, because that is what we do. If there is some way we can encourage the culture change to, I guess, exhort for more common sense, and that might be the operative word, I would like to hear instruction from our consumers.

So the floor is yours until the light is red. Governor Gilmore, do you want to take a shot at that? You have tried it from the executive side.

Mr. GILMORE. Are you asking, Congressman, where the line should be drawn between additional security——

Chairman GOSS. How much do you think we need to do in Congress to try and draw that line?

Mr. GILMORE. I think that the approach the Congress ought to take is to examine proposals for reforms, because they are coming a mile a minute now after 9/11, different proposals, structurally and otherwise, and always test those against the question of whether or not it is going to mean a loss of civil liberties in the country, or even if it has the potential for such.

For example, we have taken a great deal of time in our commission focusing on the use of the military, not because we think there is anyone evil or bad in the military anywhere, but because 50

years from now if we begin to apply the wrong kinds of structures, somewhere up the road you may run into a problem. So my advice to the Congress would be to always be taking into account the potentialities for the restrictions of civil rights and civil liberties based upon the reforms being urged upon you.

Is that responsive, Congressman?

Chairman GOSS. It is responsive. It is a very difficult question for us, as you know, and we want to understand the culture at the front lines of the working agencies and be supportive, and we want them to do their functions and understand their missions. We have given them conflicting orders. We tell one group of people this is all done on a need-to-know basis, and then we sit here and say not so fast on need to know, start to share. We understand there are conflicting signals coming out. I guess I am calling for the political courage to do the right thing based on common sense at the right moment. You can't legislate that, in my view.

Mr. GILMORE. I don't believe people on our commission feel that intelligence-sharing, either horizontally or vertically, is a challenge to the civil liberties of the country.

Chairman GOSS. You don't.

Mr. GILMORE. Now it could potentially be, but mostly it is a matter of getting proper information to people and getting them properly cleared. The danger, the more real danger is that we will put into place innovations of privacy or even law enforcement or military applications that will make us more secure, but in the end begin to impinge upon our civil liberties.

For example, within our commission we recommended, for example, that military never be first responder in a first response capacity, but always in support of a Federal civil organization, civilian organization.

We only did that as a safeguard. But we also think, by the way, that is based on a model that actually works.

Chairman GOSS. Thank you, Governor. I don't disagree with what you say. I have a slightly different opinion about how hard it is to convince Americans that vertical information flow from the bottom up may not be Big Brother getting into their lives, and vertical flow from the top down may not be Big Brother telling the locals how to do it. But I think those are things we are going to learn to accommodate as we go along.

Thank you.

Chairman GRAHAM. Thank you, Chairman Goss. Congresswoman Pelosi.

Ms. PELOSI. Thank you very much, Mr. Chairman. I know it is a long way from here to that baseball game, so I will try to make my five minutes within the five minutes. I know you will be a good chairman in that regard.

Gentlemen, again, thank you. I want to follow up on my distinguished Chairmen, both of them, their lines of questioning.

First of all, Chairman Graham, I am worried about San Diego as well. I was asking about information sharing to Mr. Andre earlier. But as Mr. Pease said, you have answered that question over and over again about why was the information not passed on.

But it is not just any city, it is a place where we have substantial military installations, and it seems to me in those cases, maybe we

have to be—of course, protection is our driving force here, especially before September 11, that perhaps we have to be more proactive where we have more exposure to know what is out there, who is going into certain places to the extent we can, when the port of entry is near those places, and certainly they are all over southern California.

So I don't know if that is possible. What I do know, following up on what Chairman Goss said, is that before we start limiting the civil liberties of the American people, we have to do what we are doing correctly. We cannot miss something that is as clear as can be and then say we need to spy more on the American people so that we can get this right.

We have to at least communicate the information that we do have. We have to collect it obviously in a more sensitive way so we know the value of it and communicate it to those who can analyze it in relationship to what else they know, where the judgment is good on it.

So I would hope, as we go forward, the easy out isn't to say we need to know more of the plans and intentions of the American people. Certainly we do. But do we have to know that by spying on them or just understanding better some of the risks of people coming in and out who have been clearly associated with those who are up to no good when it comes to terrorism in the United States.

I was interested, Mr. Greene, in what you said to Mr. Boehlert about the nonresident aliens coming into the United States—excuse me, non-immigrant aliens coming into the United States, half a billion in a year, 250 million at any given time, doubling our population?

Mr. GREENE. The half a billion is the number of transactions.

Ms. PELOSI. It could be 10 times for the same person?

Mr. GREENE. It could be commuters across the southern or northern border. It could be a Canadian coming over for milk or a job or that sort of thing. When you actually get down to the number of non-immigrant people coming in, it could be somewhere in the order of 250 million, it could be half of that. The question that he asked was how many do we have now. I don't know the answer to that. I can give you historical stuff.

Ms. PELOSI. You said—I think I wrote it down correctly—we would have to look at it in a concentrated way. Could you tell me right now how many people you have assigned to that?

Mr. GREENE. Well, there is a major NSEERS task force, gosh, between, there is something like seven or eight people just within the Headquarters interdisciplinary unit working on just building the NSEERS project. I don't know how many are working on it from the Department of Justice. There are people in Homeland engaged in the discussion.

Ms. PELOSI. Are we talking about thousands, tens of thousands? We are talking about a quarter of a billion people, half a billion maybe.

Mr. GREENE. No, it is nowhere near on that scale in terms of our team that is building the NSEERS project. It is not thousands, I know that.

Ms. PELOSI. In this regard, globalization is with us and is the future. All countries are invigorated and refreshed by the flow of peo-

ple in and out, and we don't want to impede that dynamic, what that brings to us all, whether it is trade, education, whatever it happens to be. So, again, because we miss something over here, we want to curb what is going on over here. Again, we have to make sure that people come into our country who are fully in compliance and don't come in for bad reasons unless we know about it and can stop them.

But, again, there is something to be lost if we take the easy way out, which I think in the long run is maybe not the most successful way in terms of mission success.

Mr. GREENE. I could not agree with you more, and that really does get back to Chairman Goss' question as well, about the challenge that we have. There is no agency in Washington right now that is more risk averse than the INS, I think, and part of that is really about determining precisely what we should be doing.

We believe that what we should be doing is focusing on the terrorism, and that should be the highest law enforcement priority for the INS; and that is easy when you are dealing with a watch list. It becomes much more difficult when you are dealing with that large group of people who we may not know anything about in terms of their support of terrorism, but are coming here to either support an action or to commit an action themselves. That is going to be the real challenge for us as we build toward this future. So that is the problem for us.

Ms. PELOSI. Our country is great because it is the home of the brave and the land of the free. It is great because it is a land of immigrants and we cannot damage any of that enthusiasm——

Mr. GREENE. Absolutely.

Ms. PELOSI [continuing]. As we go forward.

Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you.

Congressman Roemer.

Mr. ROEMER. I am all for getting Eleanor Hill to the baseball game to celebrate a victory and a birthday party. I want to give her plenty of time to get through the traffic to get out there.

I was just asking the Transportation Security Administration about their efforts to collaborate and share information with regard to the Ahmed Ressam case and the similarity in timers. Mr. Pease, were you at CIA aware of these similarities?

Mr. PEASE. This was actually before my tenure in the Counterterrorism Center. This tidbit has not crossed my awareness. I will check for you to see if it arrived in CTC any time in the last few years.

Mr. ROEMER. So at this point you are not aware that either checking back through cables or in getting up to speed in your new position, going back over things, after 9/11, you are not aware of having ever seen this kind of information the Transportation Security Administration had?

Mr. PEASE. I am not. I would not want to imply it did not arrive in our Headquarters and the real experts were not aware.

Mr. ROEMER. If you could get that to the committee, I would appreciate that. Thank you, Mr. Pease.

Governor, very quickly, you said, just to be clear, that you had never been briefed as Governor on security information with respect to the State of Virginia?

Mr. GILMORE. No, there was no routine to brief the Governor on this kind of activity, nor am I aware it goes on. It may happen ad hoc and incident by incident on a case-by-case basis, perhaps through the Superintendent of the State Police. But the Governor needs to be cut in.

Mr. ROEMER. I agree. This worries me a bit. Is it because of clearance problems or because we just don't have the communication and collaboration with our Governors?

Mr. GILMORE. Both.

Mr. ROEMER. So this is something we really need to address. Are we doing that right now, making sure that Governors are brought in and cleared and getting access to some of this classified information right now, or do we still have 50 Governors waiting for clearance?

Mr. GILMORE. Waiting for clearance? They are not even being cleared.

Mr. ROEMER. None of our Governors have access to this information?

Mr. GILMORE. Not that I am aware of. There may have been some changes since I left the governorship and post-9/11, but I don't think so.

Mr. ROEMER. Is that the same, Commissioner Norris, for people in positions like you, as Commissioners of police?

Mr. NORRIS. That is actually changing for us. They have provided us with applications. Mine, I now have a Secret clearance, actually through the help of CIA. There were some people helping me to push the clearances because I requested it, and a Top Secret is coming in the future.

Mr. ROEMER. Do you know how many other commissioners have Secret clearance?

Mr. NORRIS. Actually, I don't.

Mr. ROEMER. I think we would be invaluably served to get that. I think we should expedite it for the Governors of our States as well, too.

Mr. GILMORE. It probably should be almost automatic, as it is with people in the Congress. But I think that the philosophy we are approaching is there is going to come a time when this can't be ad hoc and incidental. There have to be systems set up that not only cross the horizontal lines, but also go up and down the vertical lines too, and decisions have to be made about how many people and where are they going to be placed, and what clearances they are going to have and what routine information flows up and down. It has to be a system, not an ad hoc and incidental type of arrangement.

Mr. ROEMER. As we said all day, a seamless communication system that breaks down this system of not sharing.

My green light is still on. I am all done. Thank you very much. It has been a very informative hearing.

Chairman GRAHAM. Ms. Pelosi, any further questions or comments?

I want to say on behalf of the committee how indebted we are to each of you. This has been, as several of our members have stated, one of the most informative of our hearings in large part because we had such diversity of background and perspectives on the same set of problems. That has been very illuminating.

I anticipate that this is not going to be the last time that we will ask for your assistance, because we are close to completing our hearing phase and then moving into the development of our recommendations, which, in my judgment, is the most important aspect of this inquiry. It is not enough to have some sense that you know what happened, unless you are capable of then converting that into what changes should be made in order to avoid the tragedies of September 11 occurring again.

We look forward to the opportunity to continue to draw on your insights and wisdom to help us answer those questions.

Chairman Goss.

Chairman GOSS. Nothing more, Mr. Chairman. Thank you.

Chairman GRAHAM. Congresswoman Pelosi.

Ms. PELOSI. Nothing further.

Chairman GRAHAM. Thank you very much. Now it is on to baseball.

Let me announce for our members and others that we will hold a hearing on Thursday at 10:00 a.m. in this room. The subject will be an expert panel not dissimilar from the panel we have just had. Various individuals, including former Directors of the CIA and FBI and other important intelligence agencies, as well as a former Chairman of the House Intelligence Committee, will be on the panel to give us their insights as to what should we be recommending to the American people and our colleagues for reforms.

Thank you very much.

[Whereupon, at 4:23 p.m., the joint committee was adjourned.]

STATEMENT FOR THE RECORD

SPENCER ABRAHAM

SECRETARY, DEPARTMENT OF ENERGY

JOINT INTELLIGENCE INQUIRY

UNITED STATES SENATE
SENATE SELECT COMMITTEE ON INTELLIGENCE

AND

UNITED STATES HOUSE OF REPRESENTATIVES
HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

September 20, 2002

STATEMENT FOR THE RECORD
SPENCER ABRAHAM
SECRETARY, DEPARTMENT OF ENERGY

JOINT INTELLIGENCE INQUIRY
UNITED STATES SENATE
SENATE SELECT COMMITTEE ON INTELLIGENCE
AND
UNITED STATES HOUSE OF REPRESENTATIVES
HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

September 20, 2002

Introduction

I am pleased to provide the Committees with this Statement for the Record as requested in your letter of September 17, 2002. The Department of Energy continues to make significant strides in contributing to the US government's effort to deal with the threats posed and the issues presented since the tragic events of September 11, 2001. Through the Department's intelligence, counterintelligence, and security components, the sharing of terrorism-related information within the Department and with the Intelligence and Law Enforcement Communities has improved significantly. I am personally committed to accelerating this process. The following statement reflects the outline of the specific questions posed in your letter.

Policies, Procedures and Processes for Receiving Information. National policies for the sharing of classified information are established in Executive Order (E.O.) 12958 "Classified National Security Information." Other national policies addressing cooperation among the Intelligence Community, law enforcement agencies and the Department are included in various Executive Orders and presidential directives such as Executive Order 12333, "United States Intelligence Activities," E.O. 12656, "Assignment of Emergency Preparedness Responsibilities," Presidential Decision Directive (PDD) 61, "U.S. Department of Energy Counterintelligence Program," and PDD 39 "Counterterrorism Policy," and various Director of Central Intelligence Directives (DCID). The National Security Act of 1947 (50 U.S.C. 401) also identifies roles and responsibilities of Departments and Agencies for sharing intelligence information.

These national policies are implemented through the Department of Energy's (DOE) Safeguards and Security, Counterintelligence, and Intelligence directives. Within DOE, the Office of Intelligence (IN), Office of Counterintelligence (OCI) and Office of Defense Nuclear Counterintelligence (ODNCI) are component members of the Intelligence Community (IC). The Director, IN, is the Department's Senior Intelligence Official (SIO)

and point of contact with the IC for all foreign intelligence activities; the Director, OCI, who is on detail from the FBI, is the Department's point of contact with the Federal Bureau of Investigation (FBI) for investigative referrals. As members of the IC, DOE intelligence and counterintelligence components receive foreign intelligence and counterintelligence directly through authorized IC channels. This includes relevant information concerning terrorism, suspected terrorists and their associates. E.O. 12333 implementation procedures govern departmental intelligence activities including the collection, retention and dissemination of intelligence information.

Under E.O. 12333 and the DOE Intelligence Procedures approved by the Department of Justice (DOJ), DOE intelligence and counterintelligence components are authorized to receive, retain, analyze and further disseminate law enforcement and security information relating to the Department's foreign intelligence and counterintelligence missions. In addition, the Department has in place specific procedures that authorize the sharing of information with intelligence components of law enforcement relating to DOE so that the information can be "fused" with intelligence information for timely, coordinated response to breaking events. Thus, while DOE intelligence and counterintelligence components do not collect purely domestic law enforcement/security information – i.e., without any international terrorist or other foreign connection -- they can and do receive mission-related law enforcement information from the Department's security components and outside law enforcement agencies. In turn, DOE intelligence and counterintelligence components are authorized to disseminate relevant information to the appropriate federal, state or local law enforcement agencies. The primary directive controlling the handling and dissemination of intelligence within DOE is Director of Central Intelligence Directive (DCID) 6/6, "Security Controls on the Dissemination of Intelligence Information." DCID 6/6 has been implemented at DOE in coordination with the Director of Central Intelligence (DCI) Office of General Counsel and Community Management Staff as set forth in an implementation memorandum dated January 17, 2002.

The Department primarily receives law enforcement information concerning terrorism, suspected terrorists and their associates via the National Crime Information Center (NCIC) network. That data is received and subsequently distributed to appropriate security elements within HQ and Field Elements by the DOE Office of Security (SO).

The Department receives intelligence information via Intelink and the Joint Worldwide Intelligence Communications System (JWICS), which functions as the IC classified equivalent of the Internet. Intelink allows web dissemination of all-source intelligence information, including a wide array of terrorist-related reporting and analysis. Additionally, DOE receives record message ("cable") traffic disseminated by all intelligence collection entities. Analysts in IN and technical specialists at the Field Intelligence Elements (FIEs), located at selected DOE facilities, have access to the full range of IC resources. From the law enforcement perspective, IN and the FIEs receive terrorist-related intelligence reporting generated by the FBI as part of the Intelink information flow. Subsequently, IN and FIE personnel regularly brief and supply relevant intelligence reports to appropriately cleared individuals at DOE HQ and program offices.

Joint Organizations and Information Sharing. The Department is active in several joint organizations that support counter-terrorism. Within the Intelligence Community (IC), IN is actively engaged with the Director of Central Intelligence sponsored Homeland Security Intelligence Council (HSIC). This group provides the focal point for the Office of Homeland Security (OHS) for dealing with the IC, and correspondingly provides the IC with a forum to collectively deal with those intelligence matters with which the OHS requires assistance. Such areas include information transfer issues associated with law enforcement, providing personnel resources to assist in terrorism analysis, organizational and procedural matters, and a vehicle for exchanging information on capabilities and initiatives.

IN is also an active participant in the Joint Inter-Agency Coordination Groups (JIACG), created by the Joint Chiefs of Staff following 9/11. It provides an inter-agency forum for assisting the combatant commands with the support that they require from across the US government. Activity has been greatest with the Joint Forces Command (JFCOM) and Northern Command (NORTHCOM), both of which have domestically oriented missions. A particularly noteworthy project that has been led by JFCOM, but engages all of the domestically oriented government agencies, is the Homeland Infrastructure Foundation Level Database (HIFLD) which is creating a national map supported by imagery and facilities data to be available to all federal, state, and local homeland security agencies at various levels of classification. IN's contribution to this collaboration will be to provide all energy-related data (electric grid, pipelines and nuclear facilities) as online overlays that can be applied to baseline map graphics. The result will permit all government agencies engaged in crisis or consequence management operations to have extremely detailed views of the particular area of interest during any situation.

DOE Office of Security (SO) participates in several cooperative ventures designed to support counter-terrorism initiatives. The specific objectives of the task forces and joint efforts vary, but the overall goal is to facilitate the sharing of information and develop cognizant safeguards and security programs to address potential terrorism concerns, and include:

- The Weapons of Mass Destruction Task Force (WMDTF) was established by the President and run by the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) to facilitate the sharing of information across multiple agencies and to identify potential issues and operations of concern. The primary focus is the identification of materials, operations, scenarios and corrective actions options pertaining to postulated terrorist events.
- The Postulated Threat Working Group sponsored and operated by the Defense Intelligence Agency (DIA) is an intelligence community initiative to revise the Postulated Threat as applicable to government agencies.
- The Joint Design Basis Threat Working Group (JDBTWG) is a joint DOD and DOE working group specifically formed to formulate a detailed threat statement.
- The Sealed Sources Working Group is a joint effort between the DOE and NRC with the primary function of assuring that sealed sources (such as radiological

medicines and sensing devices) are adequately protected against the Design Basis Threat postulated adversary capabilities and objectives.

- The Technical Support Working Group (TSWG) is the U.S. national forum that identifies, prioritizes, and coordinates interagency and international research and development (R&D) requirements for combating terrorism.
- The Counter-Terrorism Technology Oversight Group (CTTOG) is a joint U.S./U.K. effort to share information.
- The Non-Proliferation and Arms Control Technology Working Group (NPAC-TWG) ensures effective coordination of R&D in the areas of arms control and nonproliferation.
- The Department of Defense's Physical Security Equipment Action Group (PSEAG) is a joint program that is primarily focused on military force protection.
- The R&D Working Group (RDWG) is an interagency technology coordination committee for the U.S. security community.

CI personnel at HQ and in the field obtain data from various federal and non-federal agencies, particularly the FBI and local DOD elements. At the National level, participation in the National Joint Terrorism Task Force (NJTTF) significantly enhances information sharing efforts. CI elements have become increasingly engaged with Joint Terrorism Task Forces (JTTF), which are led by the FBI and include other federal agencies and local law enforcement organizations. In a few areas, OCI /ODNCI coordinates with the Terrorism Task Forces working under the leadership of U.S. Attorneys. OCI/ODNCI is also gaining access to some technology-supported sources such as Law Enforcement On-line. This information is then exchanged internally through the CI collateral information network (CI-NET). Depending on the information, field elements use such data for general threat awareness briefings to personnel throughout the DOE complex. OCI/ODNCI has supported FBI efforts to track suspected terrorists by reviewing lists of foreign visitors and assignees for potential matches to "watch lists" maintained by the FBI.

OCI/ODNCI personnel participate in the NJTTF, and field CI personnel participate in regional JTTF. They also work jointly with the FBI on cases on DOE personnel suspected of terrorist-related activity or DOE equities. Generally speaking, there is an open exchange of information in these forums, except for restricted portions of investigative or source information. CI normally does not have direct access to information systems that might be shared with full time JTTF personnel, nor do they have the benefit of information flow that occurs on a daily basis among those teams. The JTTF and OCI/ODNCI complementary liaison activities with federal, state, and local agencies are effective and have improved the flow of threat information. OCI also notes that the National Counterintelligence Executive (NCIX) is becoming more involved in unifying the CI communities' efforts to support the War on Terrorism. Presidential Decision Directive – 75 listed the protection of personnel and assets as one of the six core missions of the CI community. OCI is a member of the National Counterintelligence Policy Board (NACIPB), and the National Counterintelligence Operations Board (NACOB) that are led by NCIX.

The combined activities of these groups result in the opportunity to share insights, needs and information gaps, requirements and priorities, questions, potential solutions and available solutions. The level and nature of involvement ranges from national government bilateral exchanges and international conferencing to individual department or agency exchanges to specific individual technical manager interchanges. The various groups and initiatives rely on a multitude of mechanisms to facilitate the sharing of information and ideas and include the cooperative authorship of threat documents and policies, safeguards and security information, and security policies.

Integration and Access into Intelligence and Law Enforcement Agencies.

The Department of Energy has a long history of making its expertise available to other agencies to solve pressing problems, and we are particularly active in this national priority as well. Scientific and technical experts have been detailed to other key IC organizations as well as receiving liaisons from outside organizations. Not only do these exchanges provide real-time technical capabilities to the agencies that need them, but they also give IN insight into urgent or developing issues, permit better coordinated budget and programmatic approaches, and the best possible analytical assessments. IN's access is commensurate with that of those individuals with which they are working. This access is extremely significant with respect to facilitating the flow of information between agencies.

In another example, the Department has provided a detailee to FBI Critical Incident Response Group (CIRG) and weapons of mass destruction (WMD) activities. On an informal basis, DOE has a close relationship with the FBI Counter- terrorism and Threat Warning Group and has contacts within the WMD Operations Unit as well. DOE also has access to the National Law Enforcement Telecommunications System (NLETS) and Law Enforcement Online (LEO), which provide general law enforcement community information and bulletins. In addition to the FBI, DOE maintains contacts in the Secret Service, ATF, State Department, and DOD for gathering information on a case-by-case basis.

Although the Department's counterintelligence elements are not formally integrated into any other law enforcement or intelligence agency, there are three FBI personnel on detail to senior positions in the Department. During periods of heightened alert or crisis, however, CI officers are present at the FBI's Strategic Information and Operations Center (SIOC). Likewise, depending on the nature and location of the threat, field elements are prepared to shift resources to participate full-time in the regional JTTF or other similar task forces.

Information Sharing with State and Local Law Enforcement for Securing DOE Facilities.

The Department has various Memoranda of Agreement (MOA) between and among specific sites and local, state, and federal law enforcement regional offices for sharing information. Separately, state and local authorities also are increasingly reaching out to DOE and its national laboratories for assistance with WMD terrorism preparedness. The nature of the assistance being sought and provided includes education, training, and assistance with scientific and technology matters.

DOE's counterintelligence field elements have established liaison programs with local and state agencies. Information provided by these agencies to Department personnel is integrated with local threat assessments and shared with the facility managers and security personnel. Additionally, CI field units report relevant information to Headquarters where it may be reviewed, evaluated and combined with other information for further dissemination to the Intelligence Community via the standardized Intelligence Information Report (IIR) format.

DOE performs threat assessments at various DOE facilities throughout the US using the Area Threat Assessment Program (ATAP) that works with the FBI, ATF, local law enforcement entities, and others in the close geographic region around these facilities to get a general threat environment – from general criminal activity to terrorists. Integration and information sharing with state and local law enforcement agencies is reflected in the ongoing "Silent Thunder" exercise program that is designed to examine Federal, State and local law enforcement and first responders crisis management procedures in reaction to a terrorist weapons of mass destruction incident at a DOE facility.

Legal or Policy Obstacles to Sharing Information.

The single greatest obstacle to effective domestic counter-terrorism and related domestic security operations is the inability of the federal government to coordinate and use all available information and resources to collect, analyze, and disseminate timely, actionable intelligence to those individuals at federal, state, and local levels that have the ability to respond to a potential crisis or an ongoing event. The restrictions on the collection and sharing of information continue to impede the timely execution of domestic counter-terrorism operations. Some of the restrictions have been eased and there has been much discussion since 9/11 about further improvements, particularly in accelerating the pace by which these improvements are adopted. In this regard, we are hopeful that legislation to establish a Department of Homeland Security that the President can support will be passed this year.

The quality and quantity of information attenuates significantly once the area or individuals of interest are within US borders. Issues involving collection of information on US persons increasingly arise especially when an intelligence component is dealing with law enforcement information. This directly affects the ability of personnel engaged in counter-terrorism and domestic security operations by limiting their ability to provide timely, actionable intelligence to policymakers, crisis response, and consequence management personnel and organizations. This is particularly acute when the individuals

are permanent resident aliens (PRA), whose status under E.O. 12333 is the same as US citizens, or when their status is unknown, in which case the required presumption is that they are US persons, whose status is the same as US citizens. The problem is further exacerbated when intelligence tracking and analysis results in a law enforcement action that requires the information to be confiscated for further criminal investigation.

While neither a legal nor policy obstacle to information sharing, but a very real cultural limitation is the concern by many in the intelligence and law enforcement communities that shared information could quickly become part of the public domain through leaks or threat alerts. These releases could not only compromise the source(s) of the information, but also make the task of acquiring new information that much more difficult, sometimes impossible. An increasing challenge is the amount of information publicly available to potential terrorists, to include potential targets, vulnerabilities, and possible public reaction.

Information sharing with the private sector.

As the lead agency for the national energy sector, DOE's Office of Energy Assurance (OEA) established and staffed the Energy Information Sharing, Coordination, and Analysis Group (ISCG) at the National Infrastructure Protection Center (NIPC). A core element of this effort is the development of a robust energy sector information sharing and threat warning capability. This public-private partnership improves the flow of information between industry and government, as well as facilitates timely, actionable warnings to help deter or prevent physical and cyber attacks against the energy infrastructure.

As part of this process, DOE also sponsors security clearances for private sector personnel and ensures that classified specific threat information is made available to industry leaders through a collaborative effort with the FBI NIPC and FBI field offices.

DOE has started a daily assessment of the vulnerabilities of operations of energy infrastructures to identify if an attack on any single facility would create a risk of large disruptions or cascading effects. If a vulnerability is identified, the DOE staff at the NIPC will be in contact with the appropriate FBI field office, which will then work with state and local authorities to ensure proper protective measures are in place. This provides a mechanism for immediate, tailored assistance to facility security managers based on real-time information.

Since December 2001, DOE also has been working closely with industry to develop guidelines that will assist in the development of security plans and procedures to better protect the national energy infrastructure. The guidelines have been developed cooperatively with industry and our interagency partners, and will establish a baseline for the further development of security requirements, verification mechanisms, and national training standards for industry personnel. Although efforts by industry are voluntary, non-participation has not been at issue. DOE has met with senior executives from industry and

industry associations, as well as the Directors of Homeland Security from most states. DOE has also made its case for the guidelines to the National Governor's Association and the National Council of State Legislatures. Our outreach efforts, and the fact that the owners and operators worked in partnership with government to create the guidelines, have resulted in unanimous support. DOE intends to conduct vulnerability assessments and site visits to verify that industry officials are implementing the agreed upon security guidelines. The assessment teams are made up of DOE officials, other federal or state officials and the same laboratory employees who develop methodologies for use by other sectors and agencies.

The Department's Office of Energy Assurance has identified 86 critical energy sites and is leading an assessment of the 23 top critical energy assets throughout the country to provide a baseline analysis on the security of the energy infrastructure. OEA sponsored an exposition to exhibit advanced security technologies to industry and state and local government. They also have conducted a review of training already available within the federal system that is beneficial to industry and assisted in the development of customized weapons of mass destruction emergency response. Finally, the Energy Assessment program has established a cyber penetration testing capability and has conducted a cyber penetration test of the Cyber Security Penetration Testing And Supervisory Control And Data Acquisition (SCADA) systems of a major pipeline company, in coordination with the Office of Pipeline Safety. They have scheduled cyber penetration testing of the SCADA systems of both nuclear power plants, in coordination with the Nuclear Regulatory Commission, and two major electricity providers, to take place later this year.

Cultural issues that impede the flow of information.

The issue of information sharing continues to receive attention at the highest levels of government and involves many complicated aspects. DOE's Intelligence program, for example, must comply with the dissemination requirements of other IC agencies when utilizing data and analysis obtained from these agencies. These guidelines impose strict controls on information sharing with customers outside the IC which can present difficulties in the timely sharing of information. DOE has also had to redirect some of the traditional ways of thinking.

Prior to 9/11, CI efforts were focused primarily on countering the efforts of foreign intelligence collectors, while countering physical threats was largely the responsibility of our security forces. Since the attacks, we have made and are continuing to make adjustments to meet an expanded requirement for CI input to terrorist threat analysis and security planning. As a Department whose primary workforce is contractors, DOE is also working to overcome the constraints in providing threat information to non-federal personnel.

Externally, we continue to depend on the major intelligence agencies to collect and disseminate information. Within those agencies, there remain processes and procedures necessary to protect their sources and methods, as well as ensure that raw, unanalyzed

information does not drive poor decision-making. Overall, the dialectic between information sharing and protection, combined with weaknesses in the integration of intelligence information systems is always a challenge within the context of breaking events. At the field level, one needs the greatest fidelity and precision, the Department must continue to find new ways to provide the appropriate intelligence and information systems need by those responding to the local situations.

In summary, historically, the intelligence and law enforcement disciplines had a different worldview and approach to their respective tasks. Consequently, neither perceived a strong need to work closely with the other. Since the disaster of last year and the continuing threat to the homeland, those perceptions are no longer valid in either environment, nor are they any longer held by any of the participants from the Department's perspective. In the post 9/11 scenario, the lines of demarcation have blurred between the intelligence and law enforcement communities. The Department of Energy is in the process of actively breaking down the barriers that used to separate these communities, learning informational and operational needs of all participants, and searching for new opportunities for information exchange.

Central Intelligence Agency

Washington, D.C. 20505

SSCI # 2002 - 4936
LA02-0168

20 November 2002

The Honorable Bob Graham
Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

In response to your request of 25 October 2002, enclosed are the responses to the Questions For the Record (QFRs) you submitted in reference to the 1 October 2002 Joint Inquiry Committee open hearing on information sharing.

Originals of this letter and enclosure are also being sent to the Chairman and Ranking Democratic Member of the House Permanent Select Committee on Intelligence and to the Vice Chairman of the Senate Select Committee on Intelligence.

Sincerely,

Stanley M. Moskowitz
Director of Congressional Affairs

Enclosure

Congressional Questions for the Record
(25 October 2002)
Information Sharing Between Federal Government and State/Local Agencies
CIA CIO Input

1. What operating system(s) and software package(s) does your agency use for internal classified e-mail correspondence? What is the average age and processing speed of your workstations?

CIA initiated its Common Workgroup Environment (CWE) program in 1996 to promote a common suite of operating system and desktop software products for the mission. CWE is built on the Windows NT operating system. The office productivity tool used within CWE for e-mail correspondence is Lotus Notes. The Lotus Notes product has been the foundation for CIA internal e-mail and workflow applications for several years due to its flexibility, agility, and reliability in supporting our worldwide environment.

CIA is engaged in a three-year workstation recapitalization program that ensures the mission customer has effective desktop computers available for its needs. Negotiated through bulk-buy acquisition vehicles, we have been very successful in driving down the cost of each workstation while driving up the processing speed and other capabilities of the machine. The cost for a desktop workstation has dropped an average of fifteen (15) percent per year since the institution of a corporate workstation program. The desktops that will be provided in FY2003 will have a processor speed of 2.0-2.53 gigahertz, bringing the average speed of desktop workstations to 450 megahertz.

2. Do individuals in your agency have the ability from their workstations to electronically send and receive e-mails and attachments to all 12 of your sister intelligence agencies (other than by STU-III Fax)? Please identify those agencies with which you do not have this ability. For those agencies with which you can electronically communicate, please identify what special procedures or actions (if any) must be taken in order to communicate with each agency. For example, do special accounts need to be established, or special hardware or software installed?

Individuals within the CIA have readily available, desktop access to send and receive e-mails and attachments to all 12 sister intelligence agencies. Intelligence Community E-mail (ICE-mail) is available through the standard Lotus Notes desktop e-mail product; no special hardware or software is required to use ICE-mail. ICE-mail is approved to support e-mail exchanges at the Top Secret level and below.

3. Do individuals in your agency have the ability from their workstations (assuming appropriate need-to-know) to access electronically classified databases and websites at all 12 of your sister intelligence agencies? Please identify those agencies with which you do not have this ability. For those agencies with which this capability exists, please identify what special procedures or actions (if any) must be taken in order to access such intranets. For example, do special accounts need to be established, or special hardware or software installed?

Individuals within the CIA have readily available, desktop access to many electronically classified databases and websites from sister intelligence agencies. Through the CIA's intranet, called CIALink, CIA users have access to Intelink-TS and many of the resources available on Intelink-TS. IC databases that are not Web-enabled or accessible without the use of extensive add-on modules are not generally available from the standard CIA desktop; information security policy prohibits the movement of certain kinds of data, e.g., mobile code, through the firewalls separating the internal CIA network from other Top Secret, IC networks.

Access to databases or applications not allowed to freely traverse through the firewalls is made available through dedicated desktops connected directly to the appropriate network. For example, access to certain DIA databases and applications is provided through dedicated Joint Worldwide Intelligence Communications System (JWICS) workstations located around CIA.

4. What percentage of your workforce has desktop access to the open unclassified Internet?

Access to the open unclassified Internet is generally available to the CIA workforce at large. About 30 percent of the staff and contractor workforce have been issued accounts to the Agency's Internet Network.

5. Does your agency ever communicate classified information to state and local law enforcement organizations? If so, by what means is this information communicated and typically to whom?

Classified information is not usually released to state and local law enforcement organizations. The CIA will send classified material in secure channels to cleared personnel at the FBI, the Office of Homeland Security and other government agencies. The CIA will send unclassified versions of information that can then be disseminated to the public. In a national crisis, the FBI and the Office of Homeland Security will determine if the classified information should be released to uncleared personnel and the public. If the release is to be made, they will notify the originating agency of the requirement to do so. Typically they release a sanitized version.

6. What are the key policy and technical impediments to implementing an effective information architecture that facilitates information sharing between agencies?

The Intelligence Community System for Information Sharing (ICSIS) is the DCI's information technology enterprise architecture and enabling infrastructure that will provide for the sharing of critical intelligence information across all elements of the IC and the dissemination of intelligence information to both traditional and non-traditional customers, including the homeland security community. ICSIS Phase One will include the following common infrastructure enablers: DCID 6/3-compliant authentication and auditing of users accessing intelligence information, encrypted cross-Community email, secure cross-Community collaborative environments, and trusted controlled interfaces for the exchange of information across security domains. The Intelligence Community Chief Information Officer (IC CIO) will work with IC organizations to deploy priority IC databases and applications using the infrastructure and its associated ICSIS enablers for ubiquitous access to authorized users across the IC and its supported Communities.

CIA supports the ICSIS architecture. ICSIS represents the most balanced approach to sharing and protecting classified information. We support the expanded use of digital certificates to facilitate the exchange of information among appropriately cleared IC partners, customers, and colleagues. Moreover, the CIA is actively engaged in several, ICSIS-compliant projects and programs aimed at improving our ability to share information between agencies at various classification levels.

UNCLASSIFIED
DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D.C. 20340-

U-03,0010/DM-CA 9 January 2003

Honorable Pat Roberts
Chairman, Select Committee
On Intelligence
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

On 1 October 2002, Mr. Louis Andre provided testimony before the 9-11 Joint Congressional Inquiry on information sharing between federal agencies and between federal and state and local agencies.

On 6 November, the Joint Inquiry forwarded several Questions for the Record the responses to which were to facilitate its inquiry into the terrorist incidents of 11 September.

Vice Admiral Jacoby, Director of DIA, has reviewed the responses to those questions and is herewith providing them for inclusion into the official record of the proceedings.

WILLIAM R. GRUNDMANN
Chief, Congressional Affairs

DIA Response to QFRs (U)

1. Former DIA Director, Vice Admiral Thomas Wilson, told the Joint Inquiry Staff that he was never sure that he received all available intelligence information. He also said that senior Defense officials received intelligence information that his analysts did not receive. Further, the Admiral questioned what good it did for him to be aware of intelligence information that his analysts did not receive.

a. What impact, prior to 9/11, did the withholding of some intelligence information from analysts have on DIA's ability to do all-source analysis and, when necessary, provide warning reports?

The impact is impossible to quantify. Terrorism intelligence information is fragmentary and ambiguous by its very nature; relevant data is imbedded in both traditional intelligence streams and the surveillance and investigative activities of law enforcement/security elements. Missing fragments may or may not improve the fidelity of a particular analytic assessment. Analysts essentially make assessments based on three broad categories of information:

- Information that has been observed, collected, and reported ("evidentiary"),
- Historical or cataloged information about a terrorist group or individual, and
- Analytic deduction based on a range of assumptions, perspectives, and theories

Generally, as more "evidentiary" information is made available, the level of analytic confidence in the assessment's accuracy and precision increases.

We know of no instance where a reporting agency deliberately withheld information that it believed conveyed indicators of a specific or general threat. However, the full value of all-source analysis is realized when it relates ambiguous fragments of seemingly benign information to validated facts developed over time, thus extracting intelligence of potential warning value. There have been instances where reporting agencies have withheld contextual information that we believe would have contributed to a fuller understanding of the threat.

b. What agencies, in particular, tend to withhold intelligence information?

All agencies that originate ('own") information withhold some categories of intelligence, either because of operational security concerns or because it does nor meet established reporting thresholds.

c. How has that practice changed, if at all, since 9/11?

Reporting thresholds for information related to terrorism have been lowered across the community. When confronted by ambiguous information, originating agencies err on the side of disseminating rather than holding the information. Significant progress has been made toward the goal of full information sharing, including breaking down compartmental barriers imposed by operational security needs. Despite this progress, we believe there remain instances when information relevant to the analysis of the terrorist threat is withheld or distribution is limited to senior, non-analytic leadership due to reporting agencies' restrictions.

d. What initiative did DIA take to obtain all information and what was the result of that initiative?

In the immediate aftermath of the October 2000 terrorist attack on the USS COLE, DIA initiated an effort to enhance Defense intelligence terrorism analysis. While part of this initiative dealt with enhancing analytic capability, the main emphasis was on significantly expanding the amount and type of information available to the all-source analyst. Central to that initiative was DIA's proposal to establish a data repository that contained all IC and law enforcement reporting, regardless of classification, caveat, or sensitivity. No such repository existed in the IC. We pledged that we would institute any and all safeguards imposed by the data originators, to include "air-gapping" the system, to ensure the security of the data. This data repository is operational and limited data loading is underway. We are continuing to work with reporting agencies to obtain approval to incorporate all relevant information into this central secure repository.

2. We understand that DIA did not receive or was not aware of three key pieces of information concerning al-Mihdhar or al-Hazmi: 1) The August 23, 2001 CIA message to FBI, State, Customs, and INS that linked the two individuals to Usama bin Ladin and placed them in Los Angeles; 2) the August 28,2001 HQ FBI communication to the New York Field Office that linked the two individuals to USS Cole perpetrators; or 3) the June 2001 INS granting of a visa application extension to al-Hazmi at a Lemon Grove, California address.

a. Did DIA or any of the service criminal investigative organizations especially the Naval Criminal Investigative Service (NCIS), receive any or all of those three pieces of information?

DIA was neither on distribution for nor made aware of any of the three referenced reports prior to September 11, 2001. The question of whether the NCIS or other Service organizations were aware of the information should be referred to them.

b. Has anything fundamentally changed since 9/11 in terms of who has access to the databases that contained information on Hazmi and Mihdhar?

While progress has been made regarding the sharing of operational information and cables, DIA does not have full access to the information in those databases.

c. Given your understanding of the NCIS mission and capabilities, what would you have expected it to do knowing that individuals with links to Usama bin Ladin were or had been in Southern California or that there were links to known USS Cole perpetrators?

The Naval Criminal Investigative Service has operating procedures that would have guided their actions in such a scenario. This question should be referred to the NCIS.

d. Are you or the service criminal investigative services now receiving information from CIA, FBI, and INS similar to the 2001 information? If not, why not? (Rep. Bishop)

While we don't know the extent of what we don't know, we are confident there are categories of information to which DIA analysts do not have access. We are aware that some reporting is not being disseminated to our analysts or it is being restricted to senior non-analytic officials, due to reporting agencies operational security concerns. We are not in a position to question, nor would we second-guess, operational and security decisions made by reporting agencies. However, this data is not analyzed in the context of other reporting and it is not undergoing rigorous analytic review to determine validity

and to develop further insights. We renew our pledge to the reporting agencies to institute any security controls or protocols they require to place this information within our central data repository.

e. If the DIA had intelligence that a base in San Diego was threatened, could that information be shared and sent to the local police? If the local police get threat information first is that information shared with the DIA today? (Rep. Pelosi)

While any answer would be speculative and the type of information to be shared driven by the range of possible scenarios, we are certain that the basic threat information could and would be shared with the threatened party and all those involved with security in the surrounding area. DIA makes every attempt to disseminate threat information at the lowest possible classification level. Moreover, DIA has an on-going initiative to share information with state and local law enforcement organizations.

3. Current acting DIA Director Admiral Jacoby in his statement for the record said that there was a need for a paradigm shift in the ownership of information. His position is that ownership of information must reside with the analysts, not the collectors.

a. How, practically, can that shift be accomplished, given the traditional practice of collectors to provide what they perceive to be 'value-added' work by processing information into formats and categories they believe to be more useful to analysts?

Admiral Jacoby did not recommend impeding the ability of collectors to provide value-added exploitation, interpretation, and packaging of raw information. On the contrary, analysts look upon such activities as insightful and beneficial. Instead, he contended that all collected information should be subjected to a parallel process wherein the raw information – once decoupled from any source identification data that must be protected -- is subjected to additional analytic scrutiny and integrated with the wide variety of other data, assumptions, and perspectives that may differ from those held by the collectors.

b. How can the needs of the analysts be met and still accommodate those of the collectors?

As stated above, the needs of the analysts and collectors are not and should not be exclusive.

4. The Director, DIA, chairs the Senior Military Intelligence Officer's Conference (SMIOC) meetings from time to time. Over the years systemic information issues have emerged from those meetings. In September 1998 one such meeting received information briefings on the East African Terrorist Bombings and the War on Terrorism. One participant observed that there must be a "domestic piece" to emphasize FBI reporting. Another stressed that there was a "commercial piece," as well with FAA. A third representative encouraged information sharing throughout all agencies as has been done with the war on drugs. Yet another recommended a community strategy for designing a framework to study and attack terrorist organizations.

a. How is it with that this shared understanding after a critical event in 1998, by the summer of 2001 we don't seem to be much better off in working together and in sharing information? What happened in the meantime?

DIA has long been a proponent of full information sharing across the intelligence and law enforcement communities. DIA initiatives to enhance Defense terrorism analysis in early 2001 represented our most concentrated effort to increase the volume and scope of

information available to terrorism analysts. We've made steady progress. While we have not achieved all of our goals, we continue to work with counterparts in both communities.

b. There appear to be different understandings of inter-agency responsibilities at different levels. This meeting shows that senior officials talk to each other. Analysts tell our Joint Staff that they communicate constantly by secure phone, video and other means. Is the inference that middle managers aren't getting information from either below or above? How accurate is that inference? If even somewhat accurate, what is to be done about it?

In DIA, interagency responsibilities are generally understood at all levels. Concerted effort is made to ensure information flows vertically and horizontally throughout the workforce. Since DIA is an organization that is dependent on information from others – it is the raw material of our trade – understanding of inter-agency responsibilities, capabilities, and policies is an imperative at every level of our organization.

5. In January 1999, a SMIOC attendee asked about the terrorist threat and who was in charge. The issue had to do with ORCON (originator controlled) information and how distribution was controlled. The answer was that "this [issue] was not about technology but about policy which had to go all the way to an Intelligence Community Principals' Committee for approval."

a. Does it take a Principals' Committee to resolve the ORCON issue, or can the DCI, on his own recognizance take action?

The Director of Central Intelligence can make unilateral decisions on the use and implementation of the caveat.

b, Either way, what has the Community done to reduce or eliminate the ORCON caveat since 1999? Since 9/11?

The caveat remains in use. In the area of terrorism information, DIA does not contend that the ORCON caveat is an impediment to the flow of information. Those in the originating organizations charged with making release decisions are uniformly responsive and reasonable.

6. In April 1999 a SMIOC meeting was convened to receive a briefing on computer network defense. Challenges to both network defense and information sharing were listed as: law enforcement versus national security; domestic versus foreign intelligence; private versus public interests; the interagency process; and policy and legal issues.

a. That is a very clear itemization, over three years ago, of exactly the same challenges that the IC is struggling with today. Did that articulation of the issues by one agency (Defense) result in interagency examination of these issues?

While our focus over the past year has been on sharing terrorist related information, the core information sharing issues related to computer network defense are similar. I am unaware of any formal interagency examination of the issues resulting from that SMIOC discussion.

b. Either way, who is working those information-sharing issues? Who brokers competing interests? Who is in charge? Who represents the interests of concerned state and local organizations?

The DCI, by virtue of his position, is the ultimate arbiter of competing interests in the intelligence sharing area, but "disputes" are generally resolved at much lower levels between organizations. DIA represents its own and DOD's interests on information sharing issues. The Homeland Defense/Security apparatus is currently the avenue for state and local organizations.

7. In January and July 2000 a decision brief on asymmetric warfare was discussed by the SMIOC. Both the NSA and the Coast Guard representatives spoke to the legal ramifications of the portion pertaining to Homeland Defense. NSA reiterated its concern about policy and legal issues, especially regarding collection in support of Homeland Defense and terrorism. The Coast Guard cautioned that new environments and new threats might mean old rules no longer applied. A legislative review of what could be done by different organizations might be needed.

a. That was nearly three years ago. Has anyone in the Intelligence Community followed up on the Coast Guard suggestion and done a legislative review?

DIA participates as part of the larger DOD representation on Homeland Defense issues. Topics such as those identified in the question are being handled within that context.

b. What is your understanding of what are the old rules that should no longer apply and how changing these rules would impact individual rights?

DIA is subject to a range of intelligence oversight policies and procedures that impose some restrictions, most notably those pertaining to United States citizens, but we are not unduly constrained from performing our foreign intelligence or force protection missions. Laws and governing directives provide sufficient flexibility and, properly interpreted and complied with, do not inhibit our ability to share or receive information relevant to the terrorist threat.

8, In February 2001 the discussion on asymmetric warfare continued at the SMIOC. NSA stated that the FISA requirements remained a major issue. NSA continued to work the issues, but legal constraints remained an impediment. The Coast Guard observed that "[the IC] had more latitude than the lawyers were allowing," and that "if [NSA was] really going to address this issue strongly, they would have to re-evaluate several Cold War parameters and policies."

a. What has been accomplished in working these issues over the past three years? Where were we just prior to 9/11 and where are we now?

See consolidated response below.

b. Has the IC ever taken the Coast Guard's advice to seek out what the law allows and not focus on what the law does not allow?

As part of its overall effort to broaden the depth and breadth of information available to analysts, DIA has been working with the DoD General Counsel and Department of Justice and law enforcement agencies to overcome impediments to sharing FISA information as it relates to terrorism threat reporting. DIA adheres to all requisite FISA handling restrictions in accordance with U.S.C. S 1806(B).

9. Do you believe that there is a lack of information sharing because the information is classified at too high a level? If the Intelligence Community classified information at a lower level, would that help information sharing? (Rep. Castle)

The level of classification is not an insurmountable obstacle to information sharing; lowering the level would not, in itself, ensure wider sharing. Analysts who require access to terrorism information generally hold the highest levels of security clearances and are adept at "sanitizing" their analysis to ensure those who need to use it can receive it. Failure to share information is a very complex phenomenon which occurs even in areas where the information is unclassified.

United States Department of State

Washington, D.C. 20520

February 5, 2003

Dear Mr. Chairman:

Following the October 1, 2002 hearing at which Ambassador Francis X. Taylor testified, additional questions were submitted for the record. Please find enclosed the responses to those questions.

If we can be of further assistance to you, please do not hesitate to contact us.

Sincerely,

Paul V. Kelly
Assistant Secretary
Legislative Affairs

Enclosure:
As stated.

The Honorable
Bob Graham,
Select Committee on Intelligence,
United States Senate.

03799

Questions for the Record
Joint Congressional 9/11 Inquiry
Responses of the Department of State

October 31 Committee letter, Question 1:

What operating system(s) and software packages does your agency use for internal classified e-mail correspondence? What is the average age and process speed of your workstations?

Answer:

Microsoft NT 4.0 and Windows 2000 are the operating systems used in the Department of State.

The Department uses Microsoft Outlook for all internal classified e-mail correspondence.

The average age of our classified computers is approximately two years and the average processing speed is 650 Mhz.

Under the Department's ongoing modernization program, desktop equipment will be upgraded every four years.

The operating system on Bureau of Intelligence and Research computers is Windows/NT 4.0. INR uses the MSOFFICE suite with Outlook as the e-mail carrier. The average processing speed of INR computers is a gigabyte.

Questions for the Record
Joint Congressional 9/11 Inquiry
Responses of the Department of State

October 31 Committee letter, Question 2:

Do individuals in your agency have the ability from their workstations to electronically send and receive e-mails and attachments to all 12 of your sister intelligence agencies (other than by STU-III Fax)? Please identify those agencies with which you can electronically communicate; please identify what special procedures or actions (if any) must be taken in order to communicate with each agency. For example, do special accounts need to be established, or special hardware or software installed?

Answer:

The Bureau of Intelligence and Research can send and receive e-mails with attachments from all members of the intelligence community over the JWICS network. No special hardware or software is required to exchange mail with these agencies.

Questions for the Record
Joint Congressional 9/11 Inquiry
Responses of the Department of State

October 31 Committee letter, Question 3

Do individuals in your agency have the ability from their workstations (assuming appropriate need-to-know) to access electronically classified databases and websites at all 12 of your sister intelligence agencies? Please identify those agencies with which you do not have this ability. For those agencies with which this capability exists, please identify what special procedures or actions (if any) must be taken in order to access such intranets. For example, do special accounts need to be established, or special hardware or software installed?

Answer:

All Bureau of Intelligence and Research personnel have the ability to access websites and databases on Intelink from their desktops. There are websites and databases that require PKI certificates to access and INR has enabled all users identified by the sponsoring agencies with those certificates.

Questions for the Record
Joint Congressional 9/11 Inquiry
Responses of the Department of State

October 31 Committee letter, Question 4:

What percentage of your workforce has desktop access to the open unclassified Internet?

Answer:

As of January 17, 2003, 32,045 users out of the planned 43,411 users -- or 74 percent -- are connected to our Sensitive But Unclassified Network known as Open Net Plus. This network allows users to access the Internet.

In the interim, there are users who do not have access to OpenNet Plus and have other means to access the Internet, such as stand-alone computers or via separate Internet-only local area networks. Our goal is to complete connections for the workforce by mid-2003.

More specifically, in the Bureau of Intelligence and Research, approximately 70 users have desktop access to this network.

Additionally, all INR analysts have access to the open unclassified Internet through the intelligence community's Open Source Information System (OSIS).

Questions for the Record
Joint Congressional 9/11 Inquiry
Responses of the Department of State

October 31 Committee letter, Question #5:

Does your agency ever communicate classified information to state and local law enforcement organizations? If so, by what means is this information communicated and typically to whom?

Answer:

The Bureau of Intelligence and Research's TIPOFF program office (INR/TIPOFF) has no current capability or mission for data sharing with state and local law enforcement organizations. We are in discussions with the FBI on a Memorandum of Understanding to make TIPOFF's database of suspected foreign terrorists available to state and local law enforcement organizations through the FBI's National Criminal Information Center and its Violent Gang/Terrorist Organization File. This would give state and local law enforcement officials access to TIPOFF's Sensitive But Unclassified biographic information for the first time. TIPOFF currently responds, at the appropriate classification levels, to ad hoc requests (usually telephonic) from the FBI.

The Bureau of Intelligence and Research's Office of Analysis for Terrorism, Narcotics and Crime (INR/TNC) has never done so directly. Some of the threat warning products that we draft or clear on for the IICT (Interagency Intelligence Committee on Terrorism) may be downgraded at FBI and passed on to state and locals, but not at our initiative. The IICT is the IC's CT umbrella organization; it is housed at CIA/CTC and answers to the Chief of CTC.

Questions for the Record
Joint Congressional 9/11 Inquiry
Responses of the Department of State

October 21 Committee letter, Question 6:

What are the key policy and technical impediments to implementing an effective information architecture that facilitates information sharing between agencies?

Answer:

The basic technical requirements for information sharing between agencies are:

-- secure links between agency internal networks (intranets);
-- shared and searchable staff directories that include office responsibilities and contact information (including email address);and
-- agreed security standards and some basic agreement on the use of software and data applications that can work seamlessly across agency boundaries as necessary.

Interagency networks such as SIPRNET *(Secret Internet Protocol Router Network)* and OSIS *(Open Source Information System)* may be the technical means towards realizing these information sharing requirements.

Key policy questions include whether to build upon existing interagency networks, or seek to create new networks, or extend a single agency's network to others.

Information sharing will not mature rapidly without effective risk management countermeasures to enable classified information exchanges among Federal agencies in a secure environment.

JOINT COMMITTEE HEARING ON THE FUTURE ORGANIZATION OF THE UNITED STATES INTELLIGENCE COMMUNITY AND LEGAL ISSUES THE INTELLIGENCE COMMUNITY FACES IN DEALING WITH TERRORISM

THURSDAY, OCTOBER 3, 2002

U.S. SENATE, SELECT COMMITTEE ON INTELLIGENCE, AND
U.S. HOUSE OF REPRESENTATIVES, PERMANENT SELECT
COMMITTEE ON INTELLIGENCE,

Washington, DC.

The Committees met, pursuant to notice, at 10:12 a.m., in Room SH–216, Hart Senate Office Building, the Honorable Bob Graham, Chairman of the Senate Select Committee on Intelligence, presiding.

Senate Select Committee on Intelligence Members Present: Senators Graham, Rockefeller, Feinstein, Durbin, Mikulski, Shelby, Roberts, DeWine, and Thompson.

House Permanent Select Committee on Intelligence Members Present: Representatives Goss, Castle, Boehlert, Gibbons, LaHood, Hoekstra, Pelosi, Harman, Roemer, Condit, Boswell, Peterson and Cramer.

Chairman GRAHAM. I call to order the Joint Inquiry of the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.

This is the seventh open hearing of our Committees as we conduct our joint inquiry into the Intelligence Community's performance regarding the September 11 attacks. The committees have also held 11 closed hearings.

The purpose of today's hearing is to receive and review suggestions for the future organization of the United States Intelligence Community and to consider legal issues that the Intelligence Community faces in dealing with terrorism. Among other matters, we have asked our distinguished witnesses for their thoughts on the role and responsibility of the Director of Central Intelligence, the Secretary of Defense and the law enforcement community in counterterrorism and domestic intelligence programs. In that context, we have also asked that they address how proposals for the organization of domestic intelligence functions might impact on civil liberties in the United States.

Today's hearing will be in two parts. First, we will hear from Ms. Eleanor Hill, staff director for the Joint Inquiry, who will give us a presentation in relation to this portion of our inquiry. We will then hear from a panel of very impressive witnesses—our former

House colleague, Congressman Lee Hamilton; Judge William Webster; Lieutenant General William Odom; and Frederick Hitz, who I will introduce more fully after Ms. Hill's presentation.

I will now ask my colleagues if they have an opening statement. Congressman Goss?

Chairman GOSS. Thank you, Mr. Chairman. I regret that the House is in the middle of a journal vote, and our members will be back shortly. But I look forward to the input we are going to receive today. We have a very distinguished group of people, and I am very grateful they've taken the time to come forward and assist us in our efforts. Thank you, sir.

Chairman GRAHAM. Thank you, Mr. Congressman. Senator Shelby.

Vice Chairman SHELBY. Thank you, Mr. Chairman. I'll try to be as brief as I can.

Mr. Chairman, in the wake of a well-publicized series of significant intelligence failures, including the failure to prevent the bombing of the World Trade Center in 1993, the failure to prevent the bombing of Khobar Towers in 1996, the failure to anticipate the Indian nuclear test in 1998, the failure to prevent the bombings of our embassies in Africa that same year, 1998, the accidental bombing of the Chinese embassy in 1999 in Belgrade, the failure to prevent the attack on the USS *Cole* in 2000, and, of course, the failure to prevent the attacks of September 11, there has been no shortage of proposals to reform the U.S. Intelligence Community in light of that.

Most of them, Mr. Chairman, have involved variations on the theme of empowering the Director of Central Intelligence, the DCI, to exercise more real authority within the mostly Defense Department-owned Intelligence Community. Other proposals, such as one being discussed in the defense authorization conference, would empower the Pentagon by creating an Under Secretary of Defense for intelligence. All of them so far have gone nowhere.

When such ideas do not founder upon the rocks of interdepartmental rivalry and what the military calls rice-bowl politics, they simply fail to elicit much interest from an Intelligence Community that, even to this day, insists that nothing is fundamentally wrong.

Too often, serious reform proposals have been dismissed as a bridge too far by administration after administration and Congress after Congress and have simply fallen by the wayside. While very modest attempts at reform have been enacted, they've been ignored by succeeding administrations and openly defied by our current Director of Central Intelligence.

With this in mind, I asked our Committee's Technical Advisory Group, what we call the TAG, last year to undertake its own look at these issues. The TAG is a group of prominent scientists and technologists that volunteer their services to advise our Committee on very difficult technical and program management issues. And I think history shows they've done an excellent job.

We worked with them over several months on these matters, and we came to some interesting conclusions. Rather than rest our hopes for reform upon plans destined to run headlong into vested interests wedded to the current interdepartmental vision of intelligence resources or to be smothered by pained indifference from

holdover bureaucrats satisfied by the status quo, the Technical Advisory Group proposed instead that the President create something entirely new—a small, agile, elite organization with the President's personal support, dedicated wholly and single-mindedly to conducting fusion analysis.

This organization would draw upon all the information available to the federal government and use the resulting knowledge to achieve a single clear goal—dismantling and destroying terrorist groups that threaten the U.S. This, they hope, might allow meaningful reform to take place without initially having to upset entrenched bureaucratic apple carts.

They proposed, in effect, an intelligence-related version of the Manhattan Project that would take place, to some extent, outside the traditional chains of command and networks of vested interests. They suggested an approach modeled on the movie catch phrase, "If you build it, they will come." If this new venture were successful, its progress would breed further successes by gradually attracting resources and support from elsewhere, and perhaps by stimulating the intelligence bureaucracies to do more to reform themselves when faced with the success of an alternative model.

I was struck the other day, Mr. Chairman, during our hearing on information-sharing by the degree to which Governor Gilmore and our DIA witness, Mr. Andre, both echoed themes emphasized by the TAG group. They described the need for a single, all-source intelligence fusion center equipped with the latest analytical and data-mining tools and authorized to apply these tools against the whole spectrum of agency databases, even to the point of accessing so-called raw data.

I think these ideas are very much on the right track. I hope, therefore, Mr. Chairman, that these two Committees, ours and the House, in considering all the proposals for intelligence reform that have been made in recent years, will also give serious consideration to the excellent work of our TAG group and the valuable advice of some of our witnesses.

Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you very much, Senator, for a very thoughtful statement. And I particularly appreciate the recognition you've given to the outstanding work of our Technical Advisory Group and the contributions which I think their ideas, as well as the witnesses that we have and will hear, will make towards our final recommendations to the American people, to the administration and to our colleagues in the Congress.

Vice Chairman SHELBY. Thank you, Mr. Chairman.

Chairman GRAHAM. Ms. Hill.

Joint Inquiry Staff Statement
Proposals for Reform within the Intelligence Community

Eleanor Hill, Director, Joint Inquiry Staff
October 3, 2002

1

Introduction

Mr. Chairman and members of the Joint Inquiry Committee, good morning. In prior hearings, we have discussed specific factual issues and systemic problems that relate to the U.S. Government's performance regarding the events of September 11th. These have included analytical, information sharing, budgetary, and cultural issues. Today's hearing moves beyond the factual record that has been established to look toward the future and the need for reform within the Intelligence Community. Specifically, today's testimony will focus on how the Community could and should be changed to strengthen and improve the ability of the U.S. government to counter terrorist threats.

In 1947, Congress passed the National Security Act. This Act established the statutory framework for the United States Intelligence Community, including the Central Intelligence Agency (CIA) and the Director of Central Intelligence (DCI). The Act also created a semi-unified military command structure under a Secretary of Defense, and a National Security Council to advise the President.

Since then, many new organizations have been created and their missions defined in a variety of laws, executive orders, regulations and policies. During this fifty-five year period, numerous independent commissions, experts, and legislative initiatives have examined the growth and evolving mission of the Intelligence Community. Many proposals have been made to address perceived shortcomings in the Intelligence Community's structure, management, role, and mission. These have ranged from a fundamental restructuring of the Intelligence Community to tinkering with its component parts.

The earliest studies of the Intelligence Community addressed questions of efficiency and effectiveness. They included the first and second Hoover Commissions to review the Organization of the Executive Branch of the Government in 1949 and 1955; the 1949 Dulles-Jackson-Correa Report of the Intelligence Survey Group that was established to evaluate the CIA and its relationship with other agencies; and the 1975 Commission on the Organization of the Government for the Conduct of Foreign Policy, known as the Murphy Commission. The reviews and investigations of the 1970s and 1980s -- the most prominent of which were the Rockefeller Commission on CIA activities within the United States, the Senate and House Investigating Committees led by Senator Frank Church and Congressman Otis Pike, and the Iran-Contra Committees -- dealt with issues of legality and propriety. They also addressed, in varying degrees, the fundamental operating principles of the Intelligence Community.

With the end of the Cold War, both the executive and legislative branches chartered numerous additional studies to examine a variety of issues, including:

- Intelligence Community capabilities, management, and structure;
- Extent and competence of U.S. counterintelligence;
- Managerial structure of armed services and DOD intelligence components;
- DCI roles, responsibilities, authorities, and status;
- Allocation of personnel and financial resources;
- Duplication of effort within the Intelligence Community;
- Expanded use of open source intelligence; and
- Need for covert action capability.

Since the end of the Cold War in the early 1990's, the pace of reviews and studies relating to the Intelligence Community has markedly increased. The more prominent of these have included:

- 1995-1996: Commission on the Roles and Capabilities of the U.S. Intelligence Community (Aspin-Brown Commission)
- 1996: IC21: The Intelligence Community in the 21st Century (House Permanent Select Committee on Intelligence Staff Study)
- 1997: Modernizing Intelligence: Structure and Change for the 21st Century (Odom Study)
- 1998: Intelligence Community Performance on the Indian Nuclear Test (Jeremiah Report)
- 1999: The Rumsfeld Commission on the Ballistic Missile Threat
- 2000: Countering the Changing Threat of International Terrorism, a report from the National Commission on Terrorism (Bremer Commission)
- 2000: Report of the National Commission for the Review of the National Reconnaissance Office
- 2000: National Imagery and Mapping Agency Commission Report
- 2001: Road Map for National Security: Imperative for Change, The Phase III Report of the U.S. Commission on National Security/21st Century (Hart-Rudman Commission)
- 2001: The Advisory Panel to Assess Domestic Response Capabilities to Terrorism Involving Weapons of Mass Destruction (Gilmore Commission) (Third Annual Report)
- 2001: Deutch Commission on Weapons of Mass Destruction
- 2002: A Review of Federal Bureau of Investigation Security Programs, (Webster Commission)
- 2002: HPSCI Subcommittee on Terrorism Study
- Scowcroft Commission (Report not yet released)

These reviews varied in the areas they examined and emphasized different issues in their reports. However, the reports identified several areas where improvement was needed, including:

- Development of a strong national security strategy;

- Information sharing with other federal agencies and with state and local government organizations;
- Greater emphasis on human intelligence;
- Additional resources for analysts and linguists; and
- Restructuring the distribution of responsibilities and authorities between the DCI and the Secretary of Defense.

For today's hearing, we have asked the witnesses to discuss these and other issues of authority and organization in the context of the findings and recommendations of these reports. More important, we have also asked them to suggest and discuss proposals for reform that might be appropriate in light of the performance of the Intelligence Community regarding the September 11 attacks. Their testimony will, we expect, include a discussion of the role and responsibilities of the DCI, the Secretary of Defense, the law enforcement community, and the proposed Department of Homeland Security in supporting or implementing counterterrorism and domestic intelligence programs. Finally, we have solicited their thoughts on the establishment of a domestic intelligence organization and the question of to what extent such an organization could raise concerns regarding the preservation of civil liberties.

As a prelude to this morning's testimony, I would like to provide a very brief overview of a few of the previous reports on these topics and describe several common issues and themes that are of particular relevance to this Joint Inquiry.

The 1995-1996 Commission on the Roles and Capabilities of the U.S. Intelligence Community, commonly referred to as the Aspin–Brown Commission, included the following among its key findings:

- Intelligence agencies must be integrated more closely with the law enforcement community;
- Intelligence agencies must function more closely as a "Community"—there was insufficient central authority and too many administrative barriers that impeded cooperation;
- The process for allocating resources to intelligence agencies was severely flawed—workforces were not aligned to needs, multiple personnel and administrative systems were inefficient, and modern management practices needed to be utilized; and
- The confidence of the public in intelligence matters needed to be restored.

In 1996, the House Permanent Select Committee on Intelligence conducted a review of the Intelligence Community and published a staff study entitled, "IC21: The Intelligence Community in the 21st Century." Its key findings included:

- The Intelligence Community would benefit greatly from a more corporate approach to its basic functions, e.g., stronger central management, reinforced core

competencies in collection, analysis, and operations, and a consolidated infrastructure;

- The DCI required additional authorities to manage the Community as a corporate entity;
- There was little collaboration between collection agencies and all-source collection management; and
- The National Security Act and existing Executive Orders were sufficiently flexible to allow improved cooperation between law enforcement and intelligence without blurring the important distinction between the two.

General William Odom, one of our witnesses today, authored a report in 1997 entitled: "Modernizing Intelligence: Structure and Change for the 21st Century."

The report included the following observation:

"No organizational reform can overcome the absence of effective leadership and management, but dysfunctional organizational structure can neutralize the efforts of the best leaders."

The report also included the following key recommendations:

- Strengthen the role of the National Intelligence Council (NIC) in providing unique national-level analysis, and overseeing analysis and production throughout the Intelligence Community;
- Separate the Directorate of Intelligence from the CIA and subordinate it to the DCI through the NIC;
- Require the DCI to conduct a structural review of the Intelligence Community every five years; and
- Restructure CIA by giving it two major components—the national clandestine service (NCS) and a component for handling overt HUMINT. Designate the Director of this restructured organization as the national manager for HUMINT.

In 2000, the National Commission on Terrorism, led by Ambassador Paul Bremer, found that, among other things:

- The FBI, which is responsible for investigating terrorism in the United States, suffered from bureaucratic and cultural obstacles to obtaining terrorism information;
- The Department of Justice applied the statute governing electronic surveillance and physical searches of international terrorists in a cumbersome and overly cautious manner;
- The risk of personal liability arising from actions taken in an official capacity discouraged law enforcement and intelligence personnel from taking bold actions to combat terrorism;

- The U.S. intelligence and law enforcement communities lacked the ability to prioritize, translate, and understand in a timely fashion all of the information to which they have access; and
- The law enforcement community was neither fully exploiting the growing amount of information it collected during the course of terrorism investigations nor distributing that information effectively to analysts and policymakers.

Among the Commission's key recommendations were the following:

- The Attorney General should ensure that the FBI is exercising fully its authority for investigating suspected terrorist groups or individuals, including authority for electronic surveillance;
- Funding for counterterrorism efforts by CIA, NSA, and FBI must be given higher priority; and
- FBI should establish a cadre of reports officers to distill and disseminate terrorism-related information once it is collected.

Earlier this week, former Virginia Governor James Gilmore testified in detail about the work of the Advisory Panel to Assess Domestic Response Capabilities to Terrorism Involving Weapons of Mass Destruction. Chaired by Governor Gilmore, the Panel made a number of recommendations in its Third Annual Report in 2001, including:

- Increase and accelerate the sharing of terrorism-related intelligence and threat assessments with state and local governments;
- Ensure that all border agencies are partners in intelligence collection, analysis, and dissemination; and
- Increase and accelerate the sharing of terrorism-related intelligence and threat assessments among federal agencies.

Finally, in July of this year, the Subcommittee on Terrorism and Homeland Security of the House Permanent Select Committee on Intelligence, led by two members of this Joint Inquiry, Representatives Saxby Chambliss and Jane Harman, published the results of its year-long review. Among other things, the Subcommittee recommended that steps should be taken to:

- Ensure HUMINT collection remains a central core competency;
- Improve watchlisting and language capabilities;
- Ensure consumers receive the most reliable reporting and that sufficient analysis is applied; and
- Share information more completely.

Conclusion

Those are but a few of the many findings and recommendations that resulted from

many months of study and focused deliberation on the performance of the Intelligence Community. While there has been a plethora of recommendations for reform over the years, many of the most far-reaching proposals have not been acted on to any significant degree, particularly in the area of organization and structure. The tragedy of September 11th may, at long last, serve as the catalyst for action to implement meaningful and sustained reform within the Intelligence Community. We are hopeful that this Joint Inquiry will make a substantial and constructive contribution toward that end.

TESTIMONY OF ELEANOR HILL, STAFF DIRECTOR, JOINT INQUIRY STAFF

Ms. HILL. Thank you, Mr. Chairman. Good morning, Mr. Chairman and members of the joint Committees.

In prior hearings, we have, as you know, discussed specific factual issues and systemic problems that relate to the Intelligence Community's performance regarding the events of September 11. These have included analytical, information-sharing, budgetary and cultural issues.

Today's hearing, by contrast, moves beyond the factual record that has been established to look toward the future and the need for reform within the Intelligence Community. Specifically, today's testimony will focus on how the community could and should be changed to strengthen and improve the ability of the U.S. government to counter terrorist threats.

In 1947, Congress passed the National Security Act. This Act established the statutory framework for the United States Intelligence Community, including the Central Intelligence Agency and the Director of Central Intelligence. The Act also created a semi-unified military command structure under a Secretary of Defense and a National Security Council to advise the President.

Since then, many new organizations have been created and their missions have been defined in a variety of laws, executive orders, regulations and policies. During this 55-year period, numerous independent commissions, experts and legislative initiatives have examined the growth and the evolving mission of the Intelligence Community. Many proposals have been made to address perceived shortcomings in the community's structure, management, role and mission. These have ranged from a fundamental restructuring of the community to tinkering with its component parts.

The earliest studies of the community addressed questions of efficiency and effectiveness. They included the first and second Hoover commissions to review the organization of the executive branch of the government in 1949 and 1955; the 1949 Dulles-Jackson-Correa report of the Intelligence Survey Group that was established to evaluate the CIA and its relationship with other agencies; and the 1975 Commission on the Organization of the Government for the Conduct of Foreign Policy, known as the Murphy Commission.

The reviews and investigations of the 1970s and the 1980s, the most prominent of which were the Rockefeller Commission on CIA Activities within the United States, the Senate and House investigating committees led by Senator Frank Church and Congressman Otis Pike, and the Iran-Contra committees, dealt with issues of legality and propriety. They also addressed, in varying degrees, the fundamental operating principles of the Intelligence Community.

With the end of the Cold War, both the Executive and Legislative branches chartered numerous additional studies to examine a variety of issues, including Intelligence Community capabilities, management and structure; the extent and competence of U.S. counterintelligence; managerial structure of armed services and DOD intelligence components; DCI roles, responsibilities, authorities and status; allocation of personnel and financial resources; duplication

of effort within the Intelligence Community; expanded use of open-source intelligence; and need for covert action capability.

Since the end of the Cold War in the early 1990s, the pace of reviews and studies relating to the Intelligence Community has markedly increased. The more prominent of these have included—and there is a long list—in 1995 through 1996, the Commission on the Roles and Capabilities of the U.S. Intelligence Community, known as the Aspin-Brown Commission; in 1996, IC 21, the Intelligence Community in the 21st Century, which was a House Permanent Select Committee on Intelligence staff study; 1997, Modernizing Intelligence Structure and Change for the 21st Century, General Odom's study; 1998, Intelligence Community Performance on the Indian Nuclear Test, also known as the Admiral Jeremiah report; 1999, the Rumsfeld Commission on the Ballistic Missile Threat; 2000, Countering the Changing Threat of International Terrorism, a report from the National Commission on Terrorism, known as the Bremer Commission; 2000, report of the National Commission for the Review of the National Reconnaissance Office; also in 2000, the National Imagery and Mapping Agency Commission report; 2001, Road Map for National Security, Imperative for Change: The Phase III Report of the U.S. Commission on National Security in the 21st Century, also known as the Hart-Rudman Commission; also in 2001, the Advisory Panel to Assess Domestic Response Capabilities to Terrorism Involving Weapons of Mass Destruction, also known as the Gilmore Commission; in 2001, Deutch Commission on Weapons of Mass Destruction; 2002, a Review of Federal Bureau of Investigation Security Programs, also known as the Webster Commission; 2002, the House Permanent Select Committee on Intelligence Subcommittee on Terrorism report; also in 2002, the Scowcroft Commission, which has not yet released their report.

These reviews varied in the areas they examined and emphasized different issues in different reports. However, the ones we have identified, the ones we have mentioned, did identify several areas where improvement was needed, including development of a strong national security strategy; information-sharing with other federal agencies and with state and local government organizations; greater emphasis on human intelligence; additional resources for analysts and linguists; and restructuring the distribution of responsibilities and authorities between the DCI and the secretary of Defense.

For today's hearing, we have asked the witnesses to discuss these and other issues relating to the community, particularly to the authority and organization of the Intelligence Community, in the context of the findings and recommendations of those reports as well as the factual record regarding September 11 that we have seen in the course of these hearings. As a prelude to that testimony, I would like to provide a very brief overview of a few of the previous reports on these topics and describe several common issues and themes that are of particular relevance to this joint inquiry.

The 1995–96 Commission on the Roles and Capabilities of the U.S. Intelligence Community included the following among its key findings: Intelligence agencies must be integrated more closely with

the law enforcement community; intelligence agencies must function more closely as a "community." There was insufficient central authority and too many administrative barriers that impeded cooperation.

The process for allocating resources to intelligence agencies was severely flawed. Work forces were not aligned to needs. Multiple personnel and administrative systems were inefficient, and modern management practices needed to be utilized. And finally, the confidence of the public in intelligence matters needed to be restored.

In 1996, the House Select Committee on Intelligence conducted a review of the Intelligence Community and published a staff study. Its key findings included: The Intelligence Community would benefit greatly from a more corporate approach to its basic functions—for example, stronger central management, reinforced core competencies and collection, analysis and operations, and a consolidated infrastructure.

The DCI required additional authority to manage the community as a corporate entity. There was little collaboration between collection agencies and all-source collection management. And the National Security Act and existing executive orders were sufficiently flexible to allow improved cooperation between law enforcement and intelligence without blurring the important distinction between the two.

General William Odom, one of our witnesses this morning, authored a report in 1997 entitled "Modernizing Intelligence: Structure and Change for the 21st Century." The report included the following observation. "No organizational reform can overcome the absence of effective leadership and management, but dysfunctional organizational structure can neutralize the efforts of the best leaders."

The report also included the following recommendations: Strengthen the role of the National Intelligence Council in providing unique national-level analysis and overseeing analysis and production throughout the Intelligence Community; separate the Directorate of Intelligence from the CIA and subordinate it to the DCI through the NIC; require the DCI to conduct a structural review of the Intelligence Community every five years; restructure the CIA by giving it two major components—the National Clandestine Service and a component for handling overt human intelligence; designate the director of this restructured organization as the national manager for HUMINT.

In 1998, the Jeremiah report focused on the Intelligence Community's performance relating to India's testing of nuclear weapons. The report's author, Admiral David Jeremiah, noted publicly that the findings included "failures in imagination and personnel, flaws in information-gathering and analysis, and faulty leadership and training."

In 2000, the National Commission on Terrorism, led by Ambassador Paul Bremer, found that, among other things, the FBI, which is responsible for investigating terrorism within the United States, suffered from bureaucratic and cultural obstacles to obtaining terrorism information.

The Department of Justice applied the statute governing electronic surveillance and physical searches of international terrorists

in a cumbersome and overly cautious manner. The risk of personal liability arising from actions taken in an official capacity discouraged law enforcement and intelligence personnel from taking bold actions to combat terrorism.

The U.S. intelligence and law enforcement communities lack the ability to prioritize, translate and understand, in a timely fashion, all of the information to which they have access. And the law enforcement community was neither fully exploiting the growing amount of information it collected during the course of terrorism investigations nor distributing that information effectively to analysts and policymakers.

Among that commission's key recommendations were the following: The Attorney General should ensure that the FBI is exercising fully its authority for investigating suspected terrorist groups or individuals, including authority for electronic surveillance. Funding for counterterrorism efforts by CIA, NSA and FBI must be given higher priority. And the FBI should establish a cadre of reports officers to distill and disseminate terrorism-related information once it is collected.

Earlier this week, former Virginia Governor James Gilmore testified in great detail about the work of the Advisory Panel to Assess Domestic Response Capabilities to Terrorism Involving Weapons of Mass Destruction. Chaired by Governor Gilmore, the panel made a number of recommendations in 2001, including: Increase and accelerate the sharing of terrorism-related intelligence and threat assessments with state and local governments; ensure that all border agencies are partners in intelligence collection, analysis and dissemination; and increase and accelerate the sharing of terrorism-related intelligence and threat assessments among federal agencies.

Finally, in July of this year, the Subcommittee on Terrorism and Homeland Security of the House Permanent Select Committee on Intelligence, led by two members of this joint inquiry, Representatives Saxby Chambliss and Jane Harman, published the results of its year-long review. Among other things, the Subcommittee recommended that steps should be taken to ensure human collection remains a central core competency, improve watchlisting and language capabilities, ensure that consumers receive the most reliable reporting, and that sufficient analysis is applied, and share information more completely.

In sum, those are but a few of the many, many findings and recommendations that have resulted from many months of study and focused deliberation on the performance of the Intelligence Community. While there has been a plethora of recommendations for reform over the years, many of the most far-reaching proposals have not been acted on to any significant degree, particularly in the area of organization and structure. The tragedy of September 11 may at long last serve as the catalyst for action to implement meaningful and sustained reform within the Intelligence Community. We are hopeful that this joint inquiry will make a substantial and constructive contribution toward that end.

Thank you, Mr. Chairman. That concludes my statement this morning.

Chairman GRAHAM. Thank you very much, Ms. Hill. I would now like to introduce the members of our panel.

Mr. Lee Hamilton served in the House of Representatives for 17 terms, from 1965 through 1998. During the course of his outstanding service, he chaired, among other Committees, the House Permanent Select Committee on Intelligence, the House Iran-Contra Committee, and the House Foreign Affairs Committee. He is currently director of the Woodrow Wilson International Center for Scholars.

Judge William Webster, after service on the federal district and appellate benches, was the Director of the Federal Bureau of Investigation from 1978 to 1987, and the Director of the Central Intelligence Agency from 1987 until 1991. He recently chaired a Justice Department commission that examined FBI security programs in light of the espionage of Special Agent Robert Hanssen. Judge Webster now serves as a member of the President's Homeland Security Advisory Board.

General William Odom served as Director of the National Security Agency from 1985 to 1988. Prior to his tenure at the NSA, he served on the staff of the National Security Council during President Carter's administration, and then as assistant chief of staff for intelligence in the Army. General Odom is currently Director of National Security Studies at the Hudson Institute.

Frederick Hitz has served as a CIA operations officer and as director of legislative affairs at the CIA and the Department of Energy. In 1990, he was appointed as the first statutory inspector general of the Central Intelligence Agency, a position in which he served until 1998. He is currently a lecturer of public and international affairs at the Woodrow Wilson School at Princeton University.

To each of our distinguished panelists, I would like to extend our warm welcome and appreciation for your participation in this important endeavor as well as a lifetime of service to America.

Each of our committees has adopted a supplemental rule for this joint inquiry, that all witnesses will be sworn. I ask our witnesses if they would please rise at this time.

Please raise your right hand. Do you solemnly swear that the testimony that you will give before these Committees will be the truth, the whole truth and nothing but the truth, so help you God?

Mr. HAMILTON. I do.

Judge WEBSTER. I do.

General ODOM. I do.

Mr. HITZ. I do.

Chairman GRAHAM. Thank you. The prepared testimony of each witness will be placed in the record of these proceedings. I will now call on the panelists in the order in which they were introduced. First, Congressman Hamilton.

[The prepared statement of Mr. Hamilton follows:]

Testimony of the Honorable Lee H. Hamilton

Before the Senate Select Committee, House Permanent Select Committee on Intelligence
Joint Inquiry into events surrounding September 11
October 3, 2002

I. Introduction

Chairman Graham, Chairman Goss, Ranking Member Shelby, Ranking Member Pelosi, Members of the Joint Committee -- thank you for giving me this opportunity to testify before you today.

First, let me commend you for the work that you have done and for holding these hearings. You have illuminated the concerns of the nation about the events leading up to September 11, made constructive improvements in our intelligence community, and pointed the way towards further improvements.

I believe that congressional oversight of intelligence is a unique and important responsibility – the intelligence community needs strong, vigorous and thorough oversight that is independent of the executive branch. Only the Congress can provide it, and you have.

Importance of Good Intelligence

Good intelligence is essential to our national security.

We learned on September 11 that having good intelligence is as vital as it has ever been. Intelligence is the most important tool that we have in preventing terrorism, and a crucial component of our efforts to curb weapons proliferation. Policymakers simply must be able to trust that they have good intelligence as they deal with new threats – good intelligence does not guarantee good policy, but poor intelligence does guarantee bad policy.

Difficulties for the Intelligence Community

The demands on the intelligence community are huge and growing.

There are currently unprecedented demands on the intelligence community at a time when technology permits the collection of unprecedented amounts of raw data. The challenge facing the intelligence community is sifting through huge amounts of information, coordinating different agencies, and getting the right information to the right person at the right time.

Since the end of the Cold War, the dangers of international terrorism and weapons proliferation have confronted the intelligence community at a time when resources for human intelligence have decreased and priorities have been reassessed.

Need for Improvement

Currently, our intelligence capabilities are very good, but there is room for improvement.

The people working at our intelligence agencies are highly talented and dedicated to their work and country. They are called upon to do a difficult, and sometimes dangerous job, with the knowledge that good work will rarely receive outside recognition.

We have seen some spectacular intelligence successes, but we have also seen spectacular failures. Thus, it is important that we reform the intelligence community so that it is better prepared and equipped to face new and developing threats.

Reform

I am aware that too much or too little effort can be put into reform.

Too much reform can lead to spending so much time rearranging boxes that you lose sight of the mission. Too little reform can occur if key weaknesses are not addressed.

I do not favor radical change in the intelligence community, but I will suggest several reforms that would address key weaknesses in our intelligence community. I favor:

-- putting one person in charge of our intelligence community,

-- improving coordination among agencies and cooperation with foreign governments,

-- establishing a statutory foundation for the intelligence establishment,

-- increasing resources,

-- hiring more spies and expanding the talent pool,

-- increasing public understanding of the intelligence community,

-- and setting clear priorities.

I understand that several of the reforms that I will mention are already underway – my comments will re-enforce these efforts.

II. Reform

The primary purpose of our intelligence community should be advancing national security. There are many other important topics – economic, environmental and health concerns – but as we look at how to reform the intelligence community we must focus on national security.

Setting Priorities

First, we need to establish clear priorities for the intelligence community.

There is an insatiable demand for intelligence among policy-makers, and an increasing reliance on intelligence for military operations. Thus, the intelligence community is increasingly demand-driven – acting in response to requests or in reaction to events. Advances in technology complicate things by providing us with far more raw intelligence data than we could ever use – there are simply too many intelligence targets, products, and consumers.

The fact is the intelligence community cannot do everything at once and do it all well. There must be priorities established, and greater attention to long-term strategic planning. Since the end of the Cold War, there has not been a clear set of priorities or allocation of resources within the intelligence community. The National Security Council (NSC) should be clear in laying out guidelines for long-term strategic planning, and consumers must be clear in prioritizing their demands. Our two most important priorities should be:

-- combating and preventing terrorism,

-- preventing the proliferation of weapons of mass destruction.

Responsibility is on the consumers of intelligence to set, in some orderly manner, the priorities. I am not persuaded they do it – or at least do it well. Instead, they tend to demand more and more intelligence.

We must make determinations about where to focus our resources to face these new threats with a sustained and comprehensive commitment.

Organization

New intelligence priorities demand a reorganization of the intelligence community.

The very term "intelligence community" demonstrates how decentralized and fragmented our intelligence capabilities are. The intelligence community is a kind of

loose confederation. There is a redundancy in our efforts, an imbalance between collection and analysis, and problems with coordination among various agencies.

We need a center in the government for all intelligence – foreign and domestic – to come together. There is currently no place in the government where we put together data from all of our domestic and foreign sources – the CIA, FBI, Department of Defense, Department of State, NSA, and other agencies.

We need a single cabinet-level official who is fully in charge of the intelligence community – a Director of National Intelligence, or DNI. This official must be in frequent and candid contact with the president, and have his full confidence. There are very few, if any, more important presidential appointments.

The Director of National Intelligence (DNI) should have control over much, if not most of, the intelligence budget, and should have the power to manage key appointments. Currently, the Director of Central Intelligence (DCI), the leading intelligence figure, does not have this control, and thus lacks authority. In order to effectively manage the intelligence community, a Director of National Intelligence must have budget and management authority.

The Director of National Intelligence should not be the DCI, National Security Advisor or Secretary of Defense – they would have a natural bias towards their own agency. Only by establishing an independent center for intelligence with an independent, Cabinet-level official will we solve the problems of insufficient coordination and sharing of information.

The new demands on intelligence demand a new management structure. I am, of course, well aware of the opposition to this approach, and the difficulty of enacting it. But we really are in a new era, and we must think anew. If we were starting all over again, I cannot imagine we would create such a vast enterprise and have no one clearly in charge.

Improved Coordination Among Agencies

We must have better cooperation among our intelligence agencies.

We have taken steps to improve the exchange of information between various agencies since September 11, but more must be done. Turf wars and squabbling must end, and agencies including, but not limited to, the FBI, the CIA and the NSA must enhance their capability to share and coordinate intelligence.

The transnational threat of terrorism requires an unprecedented overlap between intelligence and law enforcement that presents many challenges. The CIA and the FBI have long-established roles and ways of doing things that are hard to reform, and international terrorism demands a difficult harmony between foreign and domestic operations.

Both agencies will have to fundamentally alter the way they do things in order to work together effectively. The FBI, with its new emphasis on prevention, will have to focus more on counter-terrorism, and the CIA will have to trace international leads to the homeland. Most important, the two agencies will have to share information and work together to infiltrate, disrupt and destroy terrorist cells.

To do this we will have to improve our technology. We need better computer networks to improve the flow of information within and between different agencies. For instance, there needs to be a centralized database where individual names can be checked for relevant information.

If the shortcomings leading up to 9/11 were systemic in nature, the solution lies in better system management, the handling and analysis of vast amounts of information, and the distribution in a timely manner of the key conclusions to the right people.

It is essential that the intelligence community organize itself so that all of its resources can be coordinated and agencies aid, not obstruct, one another.

Improved Cooperation with Foreign Countries

We must also develop closer intelligence relationships with countries that can help us get critical information.

Al Qaeda has operatives working in small cells in over eighty countries around the world. Material that could be used to make weapons of mass destruction can pass through global black markets. Future threats will emerge from unforeseen and remote parts of the world.

Our intelligence community cannot be everywhere at once. Already, effective cooperation with foreign intelligence has been essential in rooting out al Qaeda in the war on terrorism – countries as diverse as Pakistan, Germany, Yemen, and the Phillipines have provided assistance.

We must continue to strengthen relationships with foreign intelligence agencies to enable us to combat transnational threats.

Increased Resources

We need to substantially increase resources for the intelligence community.

In the decade following the end of the Cold War, resources for intelligence declined by some thirty percent. I am glad to see that a renewed commitment to providing resources for the intelligence community is underway – you are to be commended for that effort. We must make a sustained effort to bolster our capabilities.

We need to maintain our technological advantage, but we also must take important steps to improve our human intelligence:

--1)We need to hire more spies.

Technology alone will not make us secure. We must make a sustained commitment to putting people on the ground who can detect and alert us to terrorist plots.

New threats demand that we abandon burdensome hiring restrictions – I understand that this has already been accomplished. We will need to work within political sects and terrorist cells in countries and remote areas where we have not had a significant presence. This may demand making some unsavory contacts in order to infiltrate and break-up terrorist networks.

I do not have exaggerated expectations of what HUMINT can achieve, especially in dealing with terrorist cells. But I do believe that we must make a greater effort.

Intelligence sometimes requires unpleasant choices and human intelligence is crucial to combating terrorism. Great caution and discriminating judgments must be made.

-- 2) We need to expand the talent pool.

We must increase the number of qualified people available to our intelligence agencies. We should invest more in language and professional training. We need people who are fluent in specific and multiple languages, and people with crucial technical skills.

I understand that this effort is also underway. No one should expect quick progress here. It takes a long time to identify and train a large number of such people.

-- 3) We need to make greater use of open-source information.

We need to develop a better understanding of foreign cultures and religions. Our intelligence agencies need to make greater use of newspapers, periodicals, satellite television, radio transmissions, Internet web sites, books, pamphlets, and religious tracts that will alert us to broad trends and patterns that are developing around the world.

For years, the open-media and educational institutions in parts of the Islamic world indicated the growing level of hatred and commitment to violence against the United States. We need to pay closer attention to what the rest of the world is saying about us.

-- 4) As we increase our resources we must be cost-effective.

Merely spending more will not fix anything. We must be sure that we are getting what we pay for and what we need for the intelligence community.

Many of the steps necessary for improving our intelligence capability are not expensive.

Improving cooperation between various intelligence agencies is a matter of organization, not spending. Improved coordination and a center for intelligence should actually cut down on excessive redundancy and needless spending.

But we have to recognize that while excessive redundancy is unnecessary, some duplication is acceptable. Competing analyses and a diversity of views should be encouraged. The environment within the intelligence community must encourage analysts to speak up so that there is a constructive dialogue within and between agencies, and whistle-blowers must be comfortable in coming forward.

The intelligence community must be held to a hard-headed cost-benefit analysis – I am not sure it always has been. There is here, perhaps more than in any other area, a decided tendency to throw more dollars – and hurriedly – at the problems.

Needed improvements in human intelligence are also not a matter of major increases in spending. Human intelligence is one of the cheaper intelligence initiatives – hiring more spies and improving the talent pool are far less expensive than deploying new technologies.

If we develop an intelligence strategy based on clear priorities with a streamlined organization, we can achieve our goals while remaining cost-effective.

Respect for the Rule of Law

While advancing intelligence reforms, we must balance our need for national security with respect for the rule of law.

Reforms in the intelligence community must not come at the expense of the rule of law and respect for basic civil liberties. For instance, the coordination between intelligence and law enforcement raises important questions. Using intelligence methods must not become routine in domestic law enforcement, and the rights of U.S. citizens must be respected.

Intelligence work requires that our government obtain information, and obtaining that information requires surveillance of people who have committed no crime – the challenge is to facilitate information-gathering about suspicious people while insulating legitimate personal and political activity from intrusive scrutiny.

The U.S. intelligence agencies work within a democratic system of checks and balances. Americans want and deserve freedom and democracy, as well as effectiveness.

Congress has a major role to play in balancing the need for accountability and openness in our democracy

Statutory Foundation

We need a statutory foundation for U.S. intelligence.

U.S. intelligence is governed by a set of disparate laws and executive orders produced over the last fifty-five years. No single one of these laws provides a comprehensive legal foundation for our massive intelligence establishment. This is a remarkable state of affairs in a country that takes the rule of law so seriously.

Streamlining the intelligence community will require legislation. But we might want to go further, and try to write a legislative charter for the intelligence community. I know the difficulty of the task. Indeed, I tried to do it not once, but several times, and got nowhere. But, to me at least, it still makes sense.

Public Understanding of the Intelligence Community

We need to increase public understanding of the intelligence community.

There is much skepticism, even cynicism, about the intelligence community among the American people. It is not in our interest to let this grow, even to fester.

As much information as possible should be made public about the process, management and role of the intelligence community. Effort must be made to help the American people understand the challenges facing the intelligence community, and the manner in which those challenges are being addressed. The more the American people understand the intelligence community and the importance and difficulty of its work, the more they will trust and support the actions and policies of the government.

Politicization of Intelligence

Finally, we must be careful to ensure that intelligence is not mixed with politics. Policymakers should not use intelligence as a tool to make a policy look good – they should use intelligence as a tool to make good policy.

Because it relies so much on secrecy, intelligence fits awkwardly into an open society. Intelligence is essential to national security and secrets must be kept, but the burden is on the president and the Congress to ensure, to the maximum extent possible, that our intelligence community is held to the standards of accountability and transparency of a representative democracy.

TESTIMONY OF THE HON. LEE HAMILTON, DIRECTOR, WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS

Mr. HAMILTON. Good morning to all of you. Chairman Graham, Chairman Goss, Ranking Member Shelby and the other members of the Joint Committee, thank you very much for giving me the opportunity to join you.

I begin with a word of commendation. I know these have been very difficult hearings for the joint committee. I want you to know that I believe, particularly in the last few weeks, you have illuminated the concerns of the nation about the events leading up to September 11. I know you've already made a number of constructive improvements in the Intelligence Community. And I think you are and will point to further improvements that should be made. I'm a strong believer in congressional oversight. It's a unique responsibility of the Congress. You're the only independent oversight of the executive, and because intelligence is such an important function of government, the role of oversight is terribly important. Only the Congress can provide it effectively, and I think you have.

I will jump around in my statement. I begin with the obvious observation that good intelligence is essential to our national security. It's the most important single tool we have to prevent terrorism. Good intelligence does not guarantee good policy. Poor intelligence does guarantee bad policy.

I'm impressed by the demands that are made upon the Intelligence Community. It just seems to me they're exploding. Our technology today permits us to collect such vast amounts of information, and of course the challenge, as Eleanor Hill said a moment ago, in part is to take that information, to sift through it, coordinate the different agencies and get the right information to the right person at the right time.

Currently, I believe our intelligence capabilities are very good, but there is a lot of room for improvement. I believe that the people working on intelligence—and I've been a consumer of intelligence for over 30 years in the Congress—are highly talented and dedicated people. They are called to an extremely difficult, sometimes dangerous job, with the knowledge that good work will rarely receive outside recognition. As Senator Shelby said a moment ago, we've had some spectacular failures. We've also had some successes. But I think all of us know that we've got a lot to do to improve the Intelligence Community.

I'm very much aware that too much effort or too little effort can be put into the reform process. Too much effort can lead to spending so much time rearranging the boxes that you lose sight of your mission. Too little reform can occur if key weaknesses are not addressed. From my point of view at least, I do not favor radical change in the Intelligence Community. But I do have several reforms that I will address, and I understand that a number of these reforms are already under way, and therefore my comments will be largely to reinforce some things that have been done.

The primary purpose of the Intelligence Community is to advance the national security. There are very many important topics for intelligence to explore—economic, environmental, health concerns—but as we look at how to reform the Intelligence Community, it seems to me we have to focus on the national security.

There is just an insatiable demand for intelligence among policymakers. When I first came to the Congress, we focused principally on the Soviet missile capability, maybe the Soviet submarine capability, and that was the intelligence effort. It's a little exaggerated, but not much. Today, we simply want to know everything.

The fact is the Intelligence Community cannot do everything at once and do it all well. Priorities have to be established. Greater attention has to be given to long-term strategic planning. The House committee said in one of its reports not long ago that the focus on current intelligence erodes intelligence on comprehensive strategic analysis. I agree with that comment. There simply have to be priorities established. I'm not sure we're very good at that, those of us who have been and those who are now consumers of intelligence.

And there has not been a clear set of priorities or allocation of resources within the Intelligence Community. I understand that the National Security Council has some responsibilities in this area, but the consumers of intelligence now have to make clear to the Intelligence Community what their priorities are with regard to intelligence. From my point of view, the most important priorities at the moment are combating terrorism and preventing the proliferation of weapons of mass destruction. But the responsibility is on the consumer of the intelligence, in both the Legislative and the Executive branch to set forward in some orderly manner the priorities. And I am not persuaded that that is done today, or at least not done well. Instead, we just seem to demand more and more intelligence on every conceivable topic, and that makes it very tough on the Intelligence Community.

With regard to the organization, I favor more concentration of power in a single person. New intelligence priorities do demand a reorganization of the Intelligence Community. The very phrase "Intelligence Community" is intriguing. It demonstrates how decentralized and fragmented our intelligence capabilities are. We don't use that phrase anywhere else in the government today. The Intelligence Community is a very loose confederation. There is a redundancy of effort, an imbalance between collection and analysis, and problems, as we have repeatedly heard in recent weeks, of coordination and sharing.

We need a center in the government for all intelligence, foreign and domestic, to come together—the so-called "fusion center" idea. Senator Shelby mentioned that a moment ago in his comments. There is currently, as I understand it, no place in the government where we put it all together from the domestic and foreign services. We need a single cabinet-level official who is fully in charge of the Intelligence Community—a director of national intelligence or DNI. He must be in frequent and candid contact with the President, have his full confidence—I suspect there would be very few appointments that a President would make that would be any more important. He should have control over much, if not all, or most of the intelligence budget. He should have the power to manage the Intelligence Community.

Currently, the Director of Central Intelligence, the leading intelligence figure, as we all know does not control but a small portion of his budget. The DCI has, as I understand it, enhanced authority

after 1997, and that permits him to consolidate the national intelligence budget, to make some trade-offs, but given the overwhelming weight of the Defense Department in the process, that is of limited value.

The Director of National Intelligence should not be the DCI, the national security advisor or the Secretary of Defense. They have a natural bias towards their own agency. Secretary Rumsfeld, when he was Secretary of Defense first time around, made a comment—I don't think I can quote it exactly but I have the essence of it—he said, "if it's in my budget, I'm going to control it," and I can understand that. And that's part of the problem here in intelligence, because so much of the budget is not under the control of the top intelligence official.

So, you need a new management structure. I'm very much aware of the opposition to this approach. I'm also aware of the difficulty of enacting it. But, it's a new era, and we have to think anew. And if we were starting all over again from a blank sheet, I cannot imagine that we would create such a vast enterprise and have no one in charge, and that's what we have today. I can't think of an enterprise in America, public or private, that is so decentralized and has such little direct authority at the top.

We need more cooperation among our intelligence agencies. That's been stated repeatedly. I'll certainly not emphasize that. The principal agencies here, the FBI and the CIA, have to fundamentally alter the way they do things in order to work together more effectively. The two agencies will have to share information and work together to infiltrate, disrupt and to destroy terrorist cells. And they have to have improved technology. We need better computer networks to improve the flow of information within and between agencies. There needs to be a centralized database where individual names can be checked for relevant information.

If the shortcomings leading up to 9/11 were systemic in nature, as Ms. Hill testified a moment ago, the solution lies in better system management, the handling and analysis of vast amounts of information, and the distribution in a timely manner the key conclusions to the right people. I learned the other day that a lot of work now is being done by the Intelligence Community to check with the large private enterprises that handle vast amounts of data to see how they do it, and I suspect we've got an awful lot to learn from some of the giant enterprises in America about handling huge amounts of information.

We also have to develop a lot closer relationships with countries that can help us get critical information. We've learned that in the past few weeks. Countries as diverse as Pakistan and Germany, Yemen and Philippines have provided their assistance to us, and so we have to strengthen those relationships. Al-Qa'ida operates in 80 countries or more around the world, and we can't get all the information ourselves.

We need to increase resources for the Intelligence Community. I think a lot of this has probably already been done and that you have increased those resources dramatically, perhaps, although that figure is not public, in the last few years.

I agree with the general observations about needing to hire more spies. Technology alone will not make us more secure. I served on

the intelligence committees when we increased hugely the amount of investment in technology. We thought we were doing the right thing at the time. I think we probably were, but we did not do enough for sure with regard to human intelligence.

I think it's important, however, in the present environment that we not have an exaggerated expectation of what HUMINT can achieve, especially in dealing with a terrorist cell. I do believe we have to make a greater effort in this area, but it calls for caution and discriminating judgments. Back in the nineties, as some of us will remember, the CIA agents were closely involved with drug smugglers and human rights violators and that led to, I think it was Director Deutch, putting out guidelines with respect to hiring some people. That's been heavily criticized and I think changed in recent days. But, when you come right down to it, when you begin to hire people of unsavory reputation, it takes caution and discriminating judgement, and I'm not sure any broad guidelines can state it all for you.

But HUMINT obviously is important. We need to expand the talent pool of qualified people, language and professional training. I think that's underway. And that's not going to bring about quick progress either. It takes a long time to develop a large number of people fluent in any of these difficult languages around the world—not easy for, at least, native-born Americans—and to get them into the stream so that they're effective. That's not a quick solution. It's a very long-term one.

We need to make greater use of open-source information. On the Hart-Rudman Commission, we concluded about nine months before September 11 that Americans would die on American soil. Well, why did we conclude that? Because of terrorism. Why did we conclude that? We concluded it simply because we sensed as we traveled around the world that there was an awful lot of hostility towards Americans, a lot of resentment, a lot of anger towards us, and we began to understand that we really didn't understand very well a lot of the foreign cultures and religions. We think we're pretty nice people in this country. We can't understand why people don't like us. And we came to the conclusion that that anger had reached such a level that it would explode on us, on our soil, on some day. And, unfortunately, we turned out to be correct about that.

We have to make sure we're more cost effective in the use of resources. I said a moment ago we ought to have more resources, but merely spending does not necessarily fix anything. Many of the steps necessary for improving our intelligence capability are not expensive, and HUMINT, for example, is much less expensive than the technology that is used in intelligence gathering.

I think we have to be kind of hardheaded on cost-benefit analysis. I am not sure that we always have been in the Intelligence Community. There is here, perhaps more than in any other area that you deal with, a decided tendency to throw more dollars, and hurriedly, at the problems simply because of their urgency.

I was very pleased to see in your letter to me that you wanted a comment or two on the respect for the rule of law. Judge Webster is here. He has been one of the strongest advocates in the country for the rule of law in the FBI and in law enforcement, and I'll leave

that largely to him, except to say that the United States intelligence agencies don't operate in a vacuum. They're part of a representative democracy. They function under the United States Constitution, and they have to work within a democratic system of checks and balances.

Concluding, let me just say that we need—I believe we need a statutory foundation for the United States Intelligence Community. This extraordinary set of disparate laws and executive orders that we've produced over 55 years, none of them, I don't believe, give a comprehensive legal foundation for a massive intelligence establishment, and that is a remarkable state of affairs in a country that prides itself on taking the rule of law seriously. Now, this is exceedingly difficult to do. You're looking at a man here who tried it on three separate occasions and didn't get anywhere, so I know how difficult it is, but at least to me it still makes sense.

We need to increase public understanding of the Intelligence Community. I am now working in an environment with a lot of academics, and I am just amazed at the cynicism about the Intelligence Community that I find in the academic community. These are the people that are teaching our sons and daughters and grandchildren. It's not in our interest to let this cynicism grow. It's a tough problem. These are secret agencies. But they operate in a democratic society, and as much information as possible has to be made public about the process. And if we don't begin to educate the American people more on the Intelligence Community, the importance of the intelligence, the difficulties they confront, the obstacles they have, we're going to pay for that down the road.

And let me put a word in about politics. I'm the only politician at this table, so I have some freedom to make a comment on it, I think—a few politicians in front of me, of course.

I think we have to be careful to ensure that intelligence is not mixed with politics. Policymakers should not use intelligence as a tool to make policy look good. They should use intelligence as a tool of good policy. It's a very hard distinction to make, but it's a terribly important one. Because this community relies so much on secrecy, intelligence fits awkwardly into an open society, but it is essential to our national security. Secrets must be kept. The burden is on you, the burden is on the President, to ensure to the maximum extent possible that our Intelligence Community is held to standards of accountability and transparency as much as possible in a representative democracy.

Thank you. Thank you, Mr. Chairman.

Chairman GRAHAM. Mr. Congressman, thank you very much. Judge Webster.

TESTIMONY OF THE HON. WILLIAM WEBSTER, CHAIRMAN, WEBSTER COMMISSION

Judge WEBSTER. Thank you, Mr. Chairman. It's an honor for me to be here, and that you may be interested in some of my views. The shortness of time when I was invited to come and my travel schedule precluded me from preparing a formal statement, but if you would give me just a few minutes, I might make some informal comments and then be able to respond to whatever you might want to say.

Chairman GRAHAM. Thank you, Judge.

Judge WEBSTER. Much of what Congressman Hamilton said I find myself in total agreement with, and I will try not to repeat that. The genius of our Constitution, of our founding fathers, is in checks and balances, and over time we've been called upon to address special needs, special circumstances, but be true to our principles, including the rule of law.

In my time, when I first came here in 1978, 24 years ago, the first thing that Vice President Mondale did was to hand me a copy of the Church and Pike Committee reports with a suggestion that I read them, which I did. At that time, the pendulum had swung over in the interest of "leave us alone." Today, we have a different set of circumstances in which people are saying do something about it, and your task, along with that of the President and the judiciary—of course, I don't need to preach to the choir—is to strike that balance true, to deal with these threats as they occur, to be relevant to the particular kinds of sets we're doing, but to preserve our values and our institutions by means for which we will not have to change and upset the apple cart. I used to say, let's try to keep this pendulum as close to the center as we can, because then we'll always have to go back and change when the mood of the country changes.

General Vernon Walters, who had a distinguished career, was Deputy Director of Central Intelligence, and our representative to the United Nations, and ambassador to Germany, and trusted colleague of General Eisenhower, used to say that the American people had an ambivalent approach to intelligence. When they felt threatened, they wanted a whole lot of it, and when they didn't feel threatened, it was maybe a little immoral.

And I used to couple that with some comments about security from my perspective at the FBI. I said, "Security in this country always seems to be too much, until the day it's not enough." And this is the challenge that these great agencies which report to you for oversight have to deal with—having enough security, but not too much, and having enough intelligence, but not intruding on the rights and privacy interests of our citizens. And that's a big challenge.

And I think nowhere in my memory, in over all those years of thinking back to how we dealt with it, has there been so much impact on a problem as the issue of terrorism as it now exists in our country. In 1980, I made terrorism one of the four top priorities of the FBI. Previously there had been foreign counterintelligence, white-collar crime and organized crime. We were experiencing about 100 terrorist incidents a year, not of the size and scope of 9/11, of course, but they were killing people, they were threatening people, and they were putting people in fear.

We determined to improve our intelligence capability in order to get there before the bomb went off. And as I look back on it, I think we did a pretty good job for the nature of the challenge as it existed at that time. There were less than a handful of terrorist incidents in the year I moved from FBI to CIA in 1987. And the following year I believe there were no terrorist incidents.

There were no truly international terrorist events taking place on our shores. And that is where I think there is a significant dif-

ference that intelligence and law enforcement have to address. We had certainly—the largest terrorist events when I started were from Armenians attacking Turks in this country and from Serbs and Croatians warring with each other and Irish Republicans and so forth.

We addressed those and they disappeared from our scene. But they were not truly international terrorists as we now define them. They were people who had ties with the homelands from which they'd come or from which their parents had come. They were fighting old wars. But they were not getting their instructions and their marching orders from overseas.

This is a new experience for us, although, as I believe that Senator Shelby pointed out, the 1993 Trade Center was a wakeup call to do something about it. But it calls for new sets of relationships between CIA, which has been functioning largely abroad, until more recently, with the FBI's participation and expanded legal attache relationships, and the law enforcement responsibilities of dealing with the threat here; and now, of course, the whole concept of a new Department of Homeland Security, which will have to be dealt with in a way that advances and utilizes and magnifies the capabilities of intelligence that we have.

What I'd like to suggest—first of all, I do want to comment on the fact that President Truman, in selecting and asking for a Central Intelligence Agency, did want an agency that did not have an agenda, did not have a Defense perspective, did not have a State Department perspective, but would try to call it as they saw it to be, to provide useful and timely intelligence so that the policymakers, not the CIA, could make wise decisions in the interest of our country.

Now we're confronting what to do about terrorism. The one thought I'd like to lay on the table, and yield to the next participant and answer questions down the road, is this: More than any other kind of threat that I can recall—and I went through the Cold War and the Gulf War and the invasion of Panama and a whole host of challenges during the time I was here—more than any other kind of threat, there is an interrelationship between law enforcement and intelligence in dealing with the problem of terrorism.

At the time I started out, Interpol, the one great international organization for effective law enforcement and cooperation on an international basis, refused to authorize assistance on matters relating to terrorism because it was deemed to be an Article III type offense, which is, "We don't deal with political matters."

We worked very hard. I went to Milan. I went to Luxembourg. We dealt with the United Nations, with Interpol, and finally were able to persuade them that when you take on and injure and kill innocent victims away from the scene of the controversy, under circumstances that would be criminal in almost any other context, this was criminal, and therefore Interpol ought to cooperate and the United Nations ought to cooperate. And we moved that ball way down the road.

But I think it's important to understand it is not just criminal. It is also a matter of very good intelligence. And so it isn't enough, in my mind, to say we need more analysts to deal with the prob-

lem. In looking at these situations, we need both investigative capability and intelligence collection capability, as well as those who go through the bits and pieces and fill in the dots.

And I hope that this committee will not come up with a recommendation that tilts in one direction or the other. And you can probably anticipate I do have some views on the fact that the CIA and the FBI are now somewhat liberated from the rules that said stay away from each other that came out of the days of the Church and Pike Committee report, and that they now have a responsibility to work together and share together and not feel they're doing something that's illegal or prohibited, but also to recognize that while we talk about intelligence, investigation develops intelligence and they have to work together.

Both are important to dealing with the problem we now confront. And I hope also that in the rush to judgment, we will remember who we are and that the methods we choose, both for intelligence and for law enforcement, will be consistent with who we are in this country.

Thank you very much.

Chairman GRAHAM. Thank you, Judge Webster. General Odom.

[The prepared statement of General Odom follows:]

TESTIMONY BEFORE THE JOINT INTELLIGENCE COMMITTEE

By William E. Odom

3 October 2002

Good morning, Mr. Chairman, and members of the committee. It is an honor to appear here today.

You have asked me to share my views on the role and responsibility of the Director of Central Intelligence, the Secretary of Defense, and the FBI in dealing with terrorism. This is a very large set of topics. I have submitted a copy of an intelligence reform study, which I chaired and drafted a few years ago, as a comprehensive answer to your questions. The analysis and recommendations it puts forward, in my judgment, are all the more compelling in light of the events of 11 September 2001. I hope that this study, or parts of it, can be used as my written testimony. To be sure, I am also submitting a short additional written statement prepared especially for today to adjust the emphasis in the study to your specific interests in this hearing.

Those interests seem to be directed toward the structure of the Intelligence Community. If I am correct about that assumption, then I am encouraged. While it is important to know the details of how the intelligence failure of 11 September occurred and to assign some responsibility for it, it is far more important to take the opportunity to fix longstanding structural problems within the Intelligence Community. I certainly can offer nothing on the events leading up to 11 September of last year.

The issues of structural reform are too complex to explain comprehensively in a short statement, but it is possible to highlight three overarching issues for your attention.

The first concerns the orchestration of the intelligence process within the Intelligence Community. The second concerns management of resources, i.e., getting more intelligence for the dollar, and the third concerns counterintelligence, which is key for dealing with terrorism as well as hostile intelligence services.

Changing technology has produced a general trend in the Intelligence Community that has been delayed and blocked by bureaucratic turf concerns. Each of the three collection disciplines – signals intelligence, imagery intelligence, and human intelligence – is very different. Each needs a national manager to orchestrate collection operations.

The trend most advanced is toward a national manager in signals intelligence. The director of NSA comes close to having the authorities and means to be its national manager for signals intelligence. In imagery intelligence, the director of the NIMA is the proper candidate for that job, but his agency is very new, and his authorities and means are not yet adequate. Turf fights prevent the trend coming to fruition in imagery intelligence. In clandestine human intelligence, the CIA's Directorate of Operations has long had the authorities but shown no interest in being the national manager of the capabilities within the Defense Department.

As long the DCI is double-hatted as the director of the CIA as well, he cannot stand above the Intelligence Community and carry through the creation of fully empowered national managers for all three kinds of collection.

Turning to the second issue, getting more intelligence for the dollar, the DCI is the program manager for all the budgets within the Intelligence Community. This is potentially a very powerful authority, but given legacies within the CIA, dating back to 1947 and earlier, the CIA does not want to see its authority used for more efficiency.

Lacking national managers for the three collection disciplines and also for counterintelligence, the DCI has no subordinates who can rigorously relate inputs of resources to outputs of intelligence. His executive management organ, the Intelligence Executive Committee, includes the senior intelligence managers, but none have the control over programs that allows the DCI to hold them accountable for presenting and "Planning Program Budget" analysis, the kind that has been used in the Pentagon for forty years. If there were three national managers of the collections disciplines with full program authority over the resources spent in their disciplines, they could present a proper program budget to the DCI that shows the effects that various cuts and increases will have.

The biggest stumbling block to achieving this kind of national manager system is the National Reconnaissance Office. As a procurement organization, it spends a large part of the money allocated for signals and imagery intelligence, thus preventing the directors of NSA and NIMA from being able to trade off NRO projects against other signals and imagery projects. As long as this is the case, the waste in intelligence spending will be very large.

Finally, to the third issue, counterintelligence. It is in the worst shape of all. Five organizations run counterintelligence operations with no overall manager – the FBI, CIA, and the three military services. The parochialism, fragmentation, and incompetence are difficult to exaggerate in the US

counterintelligence world. This has become publicly clear to anyone following the reporting on the FBI and CIA over the past several months. It is not new. It has long been the case, right back to World War II and throughout the Cold War. The combination of fragmentation – which leaves openings between organizations for hostile intelligence operatives to exploit – and lack of counterintelligence skills insures a dismal performance. And terrorists, like spies, come through the openings.

The skills problem for US counterintelligence derives from mixing law enforcement with counterintelligence. Spies will always beat cops. The record of the FBI during its entire existence is a painful and irrefutable evidence of that truth. The same is true for Navy and Air Force CI, which are inside criminal law enforcement agencies.

The first step in creating an effective counterintelligence capability, therefore, is to take the CI responsibility out of the FBI, leaving the Bureau with its law enforcement responsibilities, and to create a National Counterintelligence Service (NCIS) under the DCI and with operational oversight over the CI operations of the CIA and the three military departments in the Pentagon.

This proposal has been called the "MI-5" solution, modeled on the British MI-5 organization. My version is not. It is quite different. First, a NCIS would have oversight over the CIA CI and the Pentagon CI operations, which MI-5 does not have over MI-6 and the defence ministry. Second, I would not give the NCIS arrest authority. That can be left to the FBI and other law enforcement organizations. Third, it would be under the DCI for overall program management and direction for providing CI support to all agencies of the US government, including, of course, the Department of Homeland Security.

To sum up, I propose three major reform directions:

First, separate the DCI from the Director of Central Intelligence, giving him organizational support, and create national managers for the three collection disciplines.

Second, implement a Planning Program Budgeting System within the intelligence community that better relates dollar inputs to intelligence outputs.

Third, create a National Counterintelligence Service under the DCI.

I will be delighted to take your questions and fill in details for this general picture of which there are a very large number.

TESTIMONY OF LIEUTENANT GENERAL WILLIAM E. ODOM, RET., DIRECTOR, NATIONAL SECURITY STUDIES, HUDSON INSTITUTE

General ODOM. Thank you, Mr. Chairman. Good morning—or I guess it's close to noon—members of the committee. It's an honor to appear before you today. You've asked me to share my views on the roles and responsibilities of the Director of Central Intelligence, Secretary of Defense, the FBI, in dealing with terrorism and a number of other very large topics.

I've submitted, as Eleanor Hill mentioned this morning, for your record a study I did, which is my comprehensive answer to that. The analysis and recommendations it puts forward, in my judgment, are even more compelling in light of the September 11 events of last year.

This morning I want to submit a very short statement for the record, and I will truncate it a little bit in my comments to the Committee.

Looking at this very complex set of structural issues, it's very difficult to be clear in a way that you're not implicitly introducing a lot of conflicts. But let me try to simplify in a way that I don't think—that I think removes the conflicts, because I've looked down much lower into the details here.

And I would prioritize and articulate for you three overarching structural issues. The first concerns the orchestration of the intelligence processes—some of the things Lee Hamilton mentioned here about the analytic side, not the collection side but the analysis.

The second concerns management of resources, getting more intelligence for the dollar.

The third concerns counterintelligence, which is key for dealing with terrorism as well as hostile intelligence services.

Changing technology has produced a general trend in the Intelligence Community over the last 30, 40 years, but it has been blocked and delayed in some parts of the community by bureaucratic turf concerns. Each of the three collection disciplines—signals intelligence, imagery intelligence and human intelligence, particularly clandestine—are very different disciplines. I mean, they're as different as ballet dancing, opera singing and orchestra work, and they have to be treated and handled in light of their very specific requirements.

Each, therefore, I think, needs a national manager to orchestrate the collection activities. Modern technology allows you to do that on a global scale in a way it was not possible in the 1960s. You can do things around the globe that just are not conceivable to most people if you're comparing it to the way we did it 30 years ago.

The trend here is most advanced toward a national manager system in the signals intelligence area, not because of any particular talent but because communications are their business and therefore it's somewhat to be expected. The Director of NSA comes as close to having the authority and the means to manage and orchestrate signals intelligence of anyone in the community.

Imagery—for imagery intelligence, the Director of the National Imaging and Mapping Agency is the proper candidate for that job, but his agency is fairly new. His authorities and means have not

yet been made adequate. Turf fights prevent the trend coming toward fruition in the imagery area.

In clandestine human intelligence activity, the CIA's Directorate of Operations has long had the authorities, it seems to me, in place to be a national manager if it really wanted to, but it never has shown much interest. It does its own thing by itself and has been more competitive with the Defense Department's clandestine efforts than sponsoring them the way the NSA deals cooperatively with the service cryptologic elements in the SIGINT world.

As long, I think, as the DCI is double-hatted as both the Director of Central Intelligence and the Director of CIA, it's difficult if not impossible for him to stand above the community and to carry through the creation of the fully empowered national managers for all three of these collection disciplines.

Now, turning to the second issue, getting more intelligence for the dollar, the DCI is the program manager for all these budgets. And there's a lot of power in that. I'm not sure that you have to write a new statute here. I think the DCI can exercise a lot more authority than I've ever seen any of them do. But he's blocked, to some degree, by a very powerful set of legacies, dating back to 1947 and the creation of the CIA, which does not want to see this authority used effectively in the sense that I have described it.

Since he lacks national managers in each of these discipline areas, and also for counterintelligence, which I'll turn to later, he doesn't have anybody who can rigorously relate inputs to outputs in each of these areas. His executive management organ, which I believe today is called the Intelligence Executive Committee, includes most of these senior managers.

But when that body meets, there's not a single person in that room who can say I have the program management, not necessarily budget execution, which is quite different, but program management authority from top to bottom in this discipline.

And, therefore, he cannot use the system of planning program budgeting system which was introduced in the Defense Department in the 1960s and has been there ever since, which takes line-item budgets—belt buckles, rifles, ships—separates them out, puts them behind missions, so that you can have some view of what the connection is between dollar inputs and intelligence collection outputs.

I think if there were three collection managers with full program authority, then they could be directed and I think compelled to present a budget to the DCI which shows the effects of various cuts in these disciplines. I'm leaving aside how you do this for analysis, but it's more or less the same.

The biggest stumbling block to achieving this kind of manager system is the National Reconnaissance Office. As a procurement organization, not an intelligence organization, it spends a large amount of money allocated for signals intelligence and for imagery intelligence, thus preventing the Directors of the National Security Agency and the National Imagery and Mapping Agency from being able to trade off NRO projects against other projects in each of those disciplines, which they are only in the position to know what the tradeoff would be, because they've got an information base the NRO doesn't.

And as long as this is the case, we will still have quite good intelligence, but there will be a considerable waste in input resources. In other words, if you want to improve the efficiency here—I've looked at this thing for a long time—that is the single thing that would make it possible to make gains. It won't ensure it.

Finally, the third issue is counterintelligence. I think it's in the worst shape of all. Five organizations run counterintelligence operations in the government, with no overall orchestra—conductor of the operations—the FBI, the CIA, and the three military departments.

The parochialism, fragmentation and incompetence in all are difficult to exaggerate. This has become publicly clear, I think, to anyone following the reporting on the FBI and the CIA over the past several months. It is not new. It has long been the case, right back to World War II and through the Cold War, when the NKVD ran over us like an NFL football team over a Division III football team, in the 1940s, the 1950s, the 1960s, the 1970s, the 1980s, right on down the line.

The combination and fragmentation leaves openings between the organizations which hostile intelligence operatives exploit. And also the lack of counterintelligence skills ensures a dismal performance. And terrorists are very much like spies. They come through the openings.

The skills problems that are most troubling to me here derive from mixing law enforcement and counterintelligence. Spies will always beat cops. They are a different animal. It is like—asking the cops to do the counterintelligence business is like sort of switching the personnel on the New York Yankees with the New York Giants and let the football players play baseball and the baseball players play football. They both have their competence. I don't mean to degrade any. These are just not very compatible talents. And as long as they are merged together, we will not have significant improvement of this area.

Therefore, I think the first step, if you really want to create this capability, is to create a counterintelligence organization which comes largely out of the FBI, leaves it doing its law enforcement business in the fullest sense it always has. I'd call it a National Counterintelligence Service, and I would put it under the DCI, but I would give it operational or oversight into the counterintelligence efforts of the CIA, the Army, Navy and Air Force.

And then it would be in a position to be held responsible for a comprehensive counterintelligence picture. There is no place you can get a comprehensive intelligence picture. And you will not get one by fusion center analysts. You will have to be able—you'll have to run both decentralized activities with oversight and then selective bringing back for centralization. So centralization alone is not the solution here.

Now, the proposal has sometimes of late been called the MI–5 model or solution. What I'm proposing is somewhat different. First, an NCIS, as I see it, would have oversight, as I said, over CIA and the military services, which I don't think MI–5 does over MI–6 and the defense ministry in Britain.

Second, I would not give it arrest authority. It doesn't need arrest authority. Counterintelligence is not security and it's not law

enforcement. Counterintelligence is intelligence about the enemy's intelligence. It's an operations activity to use that intelligence.

The FBI might be the agency to use it to go make the arrests and provide the evidence for prosecutions, but the business of locating spies, finding out what they're doing, understanding patentable collection, terrorist infiltrations, et cetera, can be primarily an intelligence operation.

Then the task, if you—I can see that after that was put together, then the DCI would have the responsibility to make sure it provides this kind of counterintelligence information to the agencies that need it—Homeland Security, the Defense Department, the President, the State Department and others.

Now, let me sum up briefly. I see three major reform directions. First, separate the DCI from the CIA, and at the same time create three national managers, which will mean you will have to do something, if they're going to have program authority, about the NRO.

Second, require the DCI, with its new arrangement, to implement a planning program budgeting system for handling the dollars. As I say, you won't get very far on that as long as NRO is funded the way it is. You can keep the NRO; just don't let it come to Congress for its money. Have it go to the NIMA and the NSA and say, do you need this satellite? And if you want to buy it, they'll buy it. If they don't, they don't. And they have to deliver the intelligence. And they get the phone calls if there's an intelligence failure. The head of the NRO does not get these phone calls.

Third, create a National Counterintelligence Service, as I've suggested, under the DCI. I could say more about—I worry about its potential to violate civil liberties and rights, but I think that can be managed by more oversight from the FISA courts as well as from the Congress.

That ends my remarks, and I'll be prepared to fill in the details in the question period. Thank you.

Chairman GRAHAM. Before calling on Mr. Hitz, Chairman Goss has an announcement for his members.

Chairman GOSS. I'm advised that we have a 15-minute vote right now, to be followed by a five-minute rule vote. And Members need to get themselves recorded and get back as quickly as possible so we can deal with the time constraints we've got, because additionally we're advised that those going to Hawaii this afternoon, the plane will be leaving earlier than anticipated for the funeral of Mrs. Mink, for anybody who's doing that. So I wanted to let you know we're going to be working through till 1:00, I understand.

Chairman GRAHAM. That's correct.

Chairman GOSS. Till 1:00, and we want to take advantage of the time. Thank you.

Chairman GRAHAM. Thank you, Mr. Chairman. Mr. Hitz.

[The prepared statement of Mr. Hitz follows:]

Statement of Frederick P. Hitz, Lecturer of Public and International Affairs, Woodrow Wilson School, Princeton University, before the Joint Intelligence Committee of the U.S. Senate and U.S. House of Representatives investigating the events leading to the attacks of September 11, 2001.

Thank you for inviting me to appear today. I want to talk about three disparate but connected subjects related to the way the U.S. Government goes about collecting and processing intelligence information about terrorism and terrorists. The first deals with the increasing overlap in missions between the CIA and the FBI in pursuit of the terrorist threat. The second points to several obvious ways in which statutory authority underlying the charter of the intelligence agencies to operate in this sphere must be changed to reflect the new reality. Finally, I should like to comment as a university lecturer on the appeal or lack thereof of government service to the current generation of university graduates, and what we might do about that. We all agree that terrorism will challenge the United States in some fundamentally different ways from national security threats in the past and we want our best and brightest to be drawn into this effort.

First, some scene-setting. In this short review, I am indebted to my colleague, Greg Treverton of RAND, who made remarks on this subject recently at the annual conference of the Canadian Association for Security and Intelligence Studies in Ottawa. Mr. Treverton pointed out that in the struggle against terrorism, old- fashioned distinctions between the roles of intelligence agencies such as CIA, and law enforcement such as the FBI, simply do not work. The notions that intelligence work in this area means secret, overseas and designed for the edification of policymakers exclusively no longer obtains. On the contrary, in counter terrorism operations, the CIA may be held to the evidentiary standards of the court room in terms of the

quality of its reporting. The FBI is increasingly being tasked to obtain intelligence information before the perpetration of a terrorist act, rather than merely piece together what happened and who did it after the fact. Finally, law enforcement is being challenged to meet the intelligence needs of policymakers, as well as prosecutors and the courts, and do it over the broad range of challenges that a war on terrorism entails rather than on a case-oriented basis which has been their method of operation heretofore.

This is a tall order of change for the CIA and FBI and in many ways represents the reworking of a lifetime of habits which will not happen overnight. Little wonder there has been so much talk of "connecting the dots". Considering the traditional core missions of CIA and the FBI, there have heretofore been strong reasons in both agencies never to connect the dots between them. Grand jury secrecy and prosecutorial fiat limited what FBI agents could say to others about current cases; and "need to know" and the principle of compartmentation inhibited the intelligence agencies. In addition, the National Security Act of 1947 specifically prohibited CIA from exercising "domestic law enforcement powers". Finally, the FBI and CIA have a fifty-five year history of intense rivalry and suspicion to overcome. J. Edgar Hoover sought to strangle the fledgling CIA in its crib in 1947, seeking initially to retain his overseas deployments in Latin America, and to tightly constrain CIA collection and counterintelligence activities in the U.S. even when there was a foreign nexus. As a junior clandestine services officer at CIA in the 1960s, I remember having to go through a single focal point at the FBI to obtain information: S.J. Papich. I'll never forget the name and will always wonder if there ever was such a creature. In those early days there was little chance of developing personal professional relationships and many opportunities for misunderstanding.

So I applaud the steps CIA Director George Tenet and FBI Director Robert Mueller have taken to further break down cultural barriers between the two agencies by exchanging personnel between them to work on counter terrorism. It only remains for this committee to suggest ways to streamline and rationalize the current overlap of responsibilities between the intelligence and law enforcement communities on counter terrorist matters to minimize needless rivalry and duplication of effort. I note the Attorney General has just issued guidelines governing the way grand jury testimony is to be shared with the intelligence agencies in terrorist cases under the USA PATRIOT Act. Rules of the road will have to be established in other areas affected by the Act as well. Perhaps something along those lines will be forthcoming in the surveillance area, emanating from the current appeal of the FISA Court decision to constrain the permitted use of FISA permissions in terrorist cases. Do we currently have a clear notion of how the newly expanded network of legal attaché offices abroad works with CIA Stations in the field on counter terrorist cases? These and other areas of overlapping responsibility need to be rationalized, while CIA case officers continue to learn the heightened requirements of supplying intelligence to evidentiary standards while still following unsubstantiated hunches when their gut-knowledge of the culture dictates it. Likewise, FBI agents must appreciate the value of target analysis for pre-emption purposes as well as the need to build a probative case for apprehension of the bad guys and eventual trial.

I strongly believe and have advocated in an article in the 25th anniversary issue of the Harvard Journal of Law and Public Policy last spring, that certain changes and clarifications must be sought in the laws and practices surrounding intelligence community involvement in domestic law enforcement activity as concerns counter terrorism. The most important

remaining issue, in my judgment, now that there appears to be some movement in clarifying some of the provisions of the USA PATRIOT Act on sharing grand jury testimony and FISA permissions is to amend or delete the prohibition on CIA involvement in domestic law enforcement activities contained in the 1947 National Security Act establishing the CIA. It is clear to me that with passage of the USA PATRIOT Act, if it was not manifest before, that in counter terrorism operations, CIA is sitting at the elbow of domestic law enforcement and supplying intelligence information, assistance and expertise relating to the foreign provenance of terrorist planning and implementation, as it should do if we are to be successful in preventing future 9/11 attacks. The problem is this is domestic law enforcement activity if it is intended to build a case for eventual trial in U.S. courts and is currently not permitted under the 1947 Act.

Finally, I want to say a few words touching on my current responsibilities. Each of you should be proud of the response to the events of 9/11 on the university campuses at which I teach, Princeton and the University of Virginia. I have students visiting me every day seeking help in getting their resumes to the intelligence community, law enforcement and the armed services for summer jobs, internships and permanent employment. I am supervising five undergraduate theses this year on subjects relating to the war on terrorism, historical or prospective, and have had to turn down others. Several of my students have begun the study of Arabic over the summer and are continuing it during this academic year. What concerns me is that the U.S. Government in the past has been notoriously poor in capitalizing on this outburst of patriotic enthusiasm. I read the statistics of government being overwhelmed by the growth in interest and applications for employment post 9/11 in the national security area. I can understand and

sympathize with the difficulty of dealing with the numbers. To me, however, it is so important that we capitalize on this renewed interest in public service among American students. Every person on this committee is aware of the frightening statistics reflecting the eligibility for retirement of large numbers of current federal civil servants over the next five years, with no identifiable replacement cadre in the wings. I believe Washington should respond to this quiet crisis in three dramatic ways to take advantage of the 9/11- induced interest in federal service that I see among my students:

1. Radically increase the number of summer internships that are available for qualified students in the intelligence/law enforcement arena. Students are leery about the heavy hand of bureaucracy, although they are fundamentally interested in public service. Internships allow government to look over potential new recruits without a final commitment, and more importantly, students can see how government works and get hooked on the business under the same conditions.
2. Increase federal pay. Although pay won't be the deal-breaker in most instances that keeps a student from coming to work for the feds, government salaries have slipped far below private sector salaries for the best students. Moreover, many of our ablest graduates have substantial student loans which they need to pay off, and it is clearly a factor in their decision-making, if there are other offers and the government opportunity isn't clearly overwhelming.
3. Halt the derogation of government service. For nearly a generation now, it has been a tactic common to both Republican and Democratic candidates for the highest office

in the land that Washington DC and the federal civil service have become the enemy. That view has made skeptics of my students. It is demonstrated yearly in the stats which reflect the job choices of Princeton Masters of Public Administration graduates who in significant numbers are choosing work with Non-Govenmental Organizations, NGOs, or international organizations such as the World Bank, over the U.S. Government! They want to work in the public sector but are afraid of what they believe the Washington bureaucracy has become. This misapprehension must be corrected and the patriotic climate created in the aftermath of 9/11 is the perfect time in which to attempt it.

Thank you for allowing me to express my views.

TESTIMONY OF FREDERICK HITZ, DIRECTOR, PROJECT ON INTERNATIONAL INTELLIGENCE AND LECTURER OF PUBLIC AND INTERNATIONAL AFFAIRS, PRINCETON UNIVERSITY

Mr. HITZ. Thank you, Mr. Chairman. And it's a pleasure to be back here to see so many familiar faces on the dais and behind the dais.

In the interest of time, I'm going to, as my predecessors have done, skip around in the prepared statement that I have submitted for the record. I sought in my statement to make three disparate but connected points.

First, I wanted to deal—and Judge Webster talked a little bit about it—with the increasing overlap in missions between CIA and FBI. Secondly, I wanted to talk a little bit about the way the statutory authority underlying the charter of the intelligence agencies needs to be changed to reflect the new reality of involvement in terrorist operations that extend into the United States. And thirdly, I just wanted, out of the realm of all of the discussion of structural changes, to give you a feel for how public service is looked at in the educational institutions with which I'm involved, because I think we all recognize that there are lots of things that we have to do at the current time, but in the long-term it's going to be the appeal of government service to our best and brightest citizens that will help us solve these problems.

First, as you know—and I have personal experience with this, as does, I think, Chairman Goss—the notion that intelligence work meant secret, overseas, and designed for the edification of policymakers exclusively no longer obtains. On the contrary, in counter terrorism operations, CIA increasingly has to be held to the evidentiary standard of the courtroom in terms of the quality of its reporting, because in the courtroom a number of its findings may well be tested.

Conversely, the FBI one used to think of as almost exclusively involved in domestic law enforcement activity. And now, in the effort to combat terrorism, we are asking the Bureau to act before the perpetration of a terrorist act rather than merely try to piece together what happened and who did it after the fact. In that sense, law enforcement is being challenged to meet the intelligence needs of policymakers to figure out in advance of an event what needs to be done, as well as satisfy the prosecutors and the courts, to whom they have always been bound. Its methodology will be tested over the broad range of challenges that a war on terrorism entails, rather than on a case-oriented basis, which has been their method before.

This is a tall order of change for CIA and FBI and in many ways represents the reworking of a lifetime of habits, which will not happen overnight. Little wonder there has been so much talk of connecting the dots. Considering the traditional core missions of the Agency and the FBI, there have heretofore been strong reasons in both agencies never to connect the dots between them. Grand jury secrecy and prosecutorial fiat limited what FBI agents could say to others about current cases, and need-to-know and the principle of compartmentation inhibited the intelligence agencies as well.

In addition, the National Security Act of 1947 specifically prohibited, and, as Judge Webster said, Harry Truman wanted—Presi-

dent Truman wanted some centralization of the intelligence information that was presented to him, but the history books show that he most clearly did not want to create another Gestapo, as he put it. And so, in the '47 Act, CIA was specifically prohibited from exercising domestic law enforcement powers.

And here is something to which I could speak—can speak from personal witness. FBI and CIA, up until the last several years, have a 55-year history of intensive rivalry and suspicion to overcome. FBI Director J. Edgar Hoover sought to strangle the fledgling CIA in its crib in 1947, sought to keep its authority to retain overseas deployments in Latin America, and to tightly constrain CIA collection and counterintelligence activities in the United States, even in the early days when there was a foreign nexus. As a junior clandestine services officer at CIA in the 1960s, I remember having to go through a single focal point at the FBI to obtain information. Mr. S.J. Papich—I will never forget the name, and will always wonder if there was ever such a creature. In those days, it was hard to think of establishing a day-to-day working operational relationship.

Well, those things have changed, of course. And I applaud the efforts of Director Tenet and Director Mueller to breakdown the cultural differences between the two organizations and to have CIA analysts serve on detail at the FBI and vice versa. But, it will take time.

My second point was that, and it seems that we appear to be making some progress in this world, the USA PATRIOT Act required Attorney General guidelines, for example, to implement the grand jury testimony sharing that's to take place with intelligence officers. I gather those are out. I haven't had a chance to study them. Likewise, we're going through a process that eventually will sort out what will be the area of permitted operation of the FISA court.

But, I've argued in an academic journal last spring that I think this committee and other committees of the Congress will have to come to grips with the fact that the prohibition in the '47 Act against CIA exercising domestic law enforcement powers is no longer applicable. It seems to me that with CIA, for example, sitting at the elbow of domestic law enforcement and supplying intelligence information and expertise relating to the foreign provenance of terrorist planning and implementation—which we want it to do, what it has to do if we are to be successful in preventing future 9/11 attacks—this has got to be construed, or will be construed eventually in a court of law to be domestic law enforcement activity, which is specifically prohibited currently under the 1947 Act. So, I think you have to take a look at that.

Finally, let me take a moment to talk about what I encounter on the university campus. I was sorry to hear from my distinguished colleague Lee Hamilton that his contacts or his involvement with academics have uncovered a cynical vein in the atmosphere and in the attitudes of some academics in conveying their views on the Intelligence Community at the current time. I can't say I've run into that myself, but it's perhaps a different place.

I think you would be proud of the response to the events of 9/11 that have taken place on the university campuses where I

have the privilege of teaching—Princeton and the University of Virginia. I have students visiting me every day seeking help in getting their resumes to the Intelligence Community, law enforcement, and the armed services for summer jobs, internships and permanent employment. I'm currently supervising five undergraduate theses on subjects relating to the war on terrorism, historical or prospective, and have had to turn down others. Indeed, one of my students is here today, I'm glad to say.

And several of my students over the summer have begun the study of Arabic and are continuing it during this academic year. Clearly, it's a response to the events of last year, and Arabic is not an easy language to study, as you all know.

What concerns me is that traditionally the United States government has been quite poor in capitalizing on this outburst of patriot enthusiasm. I read the statistics of government being overwhelmed by the growth in interest and number of applications for employment in the post–9/11 era in the national security area, and I can sympathize with the difficulty of sorting through these numbers. They're drinking from a fire hose. However, to me it is so important that we capitalize on the renewed interest in public service that I see among American students.

Every person on this committee is aware of the frightening statistics reflecting the eligibility for retirement of large numbers of current federal civil servants over the next five years, with no identifiable replacement cadre in the wings. I think—and perhaps these are just hobby horses, but I've had some experience with thinking through some of them—Washington should respond to this quiet crisis in three dramatic ways to take advantage of the post–9/11 interest in federal service.

Radically increase the number of summer internships that are available for qualified students in the intelligence and law enforcement area. Now these students obviously are going to be green as grass, and aren't going to be able to help out in any material way with a lot of the problems that our current CIA and FBI officers are facing, but it is so important for them to get an idea of what this work is about. It's also important for government to be able to look over these fresh faces to see if they have what it takes to work in this area, and I think internships are a perfect answer to that.

The implications of federal pay I'm sure have been brought to your attention constantly. Federal pay has fallen way behind pay in the private sector for our best students. Now that's not to say that our ablest students who are interested in government service are going to be absolutely deterred from coming in given that discrepancy, but frankly, I recognize that with the rise in cost of university education and graduate school, it means that a good many have loans to pay off, and it is a discouraging factor.

And finally, on a more general point, and I think we're all about this now, over a considerable period of time, several decades, I think it has been customary for competitors for the highest office in the land to denigrate the federal service and denigrate the U.S. government in Washington. Frankly, this has had its impact on many of the students with whom I am involved. It's made them

skeptics, and it has caused them to shy away from the federal service. Let me give you an example.

Over a five-year period, I have looked at the statistics related to the jobs that graduates of Princeton's master's in public administration program migrate to after they've finished their degree. This is a two-year degree, very intensive, involving a lot of quantitative analysis, and one which is extremely well-funded from the standpoint of students not having to pay much by way of tuition. A master's in public administration degree is utilizable in the best and most practical way by giving one's service to government. We're down around 20 percent of that graduating class, a graduating class of 63, who elect to go to work for the federal government or state, local and municipal governments. Does that mean that the rest are trucking off to Wall Street and the management consultancies? No. In many instances they are preferring NGOs, non-governmental organizations, and international work, international consultancies to these jobs. So it isn't something that can be discussed entirely in the context of money.

And I hope we're going to turn that around in our country. I think, as I say, there has been quite a patriotic response to the events of 9/11, but all of us have to work on the business of making government service in these critical areas even more attractive.

Chairman GRAHAM. Thank you very much, Mr. Hitz. As we were planning for this hearing today, we gave this hearing the title of "The Wise Men," wishing to hear people who had decades of experience with the issues that we are confronting. Our definition of this panel was too modest and I wish to thank you very much for the very significant contribution that you have made.

It has been our practice in our previous hearings to designate lead questioners who have prepared themselves to ask questions in areas of particular importance to the committee. After the lead questioners, we will then have five-minute questions from the individual members of the committee. The lead questioners, with 20 minutes each, are Senator Rockefeller, Representative Everett, Senator DeWine, and Representative Condit.

Senator.

Vice Chairman SHELBY. Mr. Chairman.

Chairman GRAHAM. Yes, Senator Shelby.

Vice Chairman SHELBY. We've been notified we have a vote on the Senate floor.

Chairman GRAHAM. It just started. If that's going to result in Senator Rockefeller having his 20 minutes interrupted, Senator, would you like to break now, vote, and then come back and you'll have your 20 minutes uninterrupted?

We will recess for the Senate vote. Hopefully also our House colleagues will have completed their votes and you'll have a larger, more attentive audience when we return. So the meeting is recessed at the call of the chair.

[Whereupon, from 11:36 a.m. until 12:00 p.m., the Committees recessed.]

Chairman GRAHAM. The Joint Inquiry has reconvened. Our first designated questioner will be Representative Everett.

Mr. EVERETT. Thank you, Mr. Chairman. And thank you, panel, for being here. Great admiration for all of you.

You know, in reading over the material and studying this, this is something we've been trying to pen up for at least 10 years or more, and I don't think we've got that rabbit penned yet. How we do it is, of course, the big question.

Let me start with the DCI and ask each of you to respond to that. Do you believe the DCI position needs to be elevated and separate from the CIA? I know that somebody has already testified to that. But I tell you, let's start with, on the left, if you don't mind, and just go right down the line. General Odom.

General ODOM. I think he should be separated. I don't see it so much as an elevation as it is a separation. It may have the appearance of an elevation if he does that, but I think he becomes trapped, the DCI becomes trapped if he's also directing an agency, and therefore he doesn't look at the community as a whole as much as he could. And I don't think things will improve much in the direction that I'm talking about until you make that separation. How much additional authority you give him, I think that's kind of—that's a variable boundary. You might want to do more or less.

My own view is that as the authorities now stand, the DCI, if he moved out, and he has to take some organizational capability with him—he can't just stand out there in an office and be a czar over in the White House. I would have an expanded National Intelligence Council, a rump part of the DI at CIA as sort of a reinforcement for him, to focus in on problems such as terrorism that other people are not focusing on or neglected. And then you'll find out, when he gets it going, other people will take it over and begin to do it sort of in a routine way. And that would give him—and then his community management staff, he would have a pretty good organizational base, and he controls the programs of all these people.

I'm not sure you can give him budget execution unless you in Congress rewrite the whole regulations for spending money in the various departments, because the Defense Department has expenditure rules. The Treasury Department has different ones. Other people have different ones. And, I don't—it seems to me that's just an administrative hurdle you have to deal with. But it's not all that critical if the exercise of program management authority is vigorously exercised.

Mr. EVERETT. But you would advocate keeping budgets separate, budget authority?

General ODOM. Well, I'd leave the budget—I don't know how you would change the budget execution. That is, after the appropriation has gone out of here and been signed into the law by the President, you give the intelligence agencies authority to spend their money. NSA is in the Defense Department; it has to spend by Defense Department rules. And I don't see how—I mean, maybe you could change that and put it under a central authority, I'm not really sure. But it strikes me that that works pretty smoothly anyway, that where the real problem comes is in the program bill side and the program presentation to the Hill, and what's hidden behind it, whether in the input-output relationships are clear there.

Mr. EVERETT. Congressman Hamilton.

Mr. HAMILTON. Congressman Everett, I go back for decades, really, and we've been talking about the DCI and the authority the DCI should have. And I think the general trend line has been that

we want to increase the authority of the DCI. And I think in 1997 he was in fact given enhanced authority. I don't discount that, but I really don't think that's the solution either.

I think the solution is to have one person, a director of national intelligence, who is over the entire Intelligence Community. That person should not be the DCI, he or she should not be the defense secretary, or he or she should not be the national security advisor. But I really think it's necessary now, given the importance of intelligence, and for accountability purposes, that you have a person who is identified as being the top person in the government on intelligence to whom you can look and you know he has the authority in terms of management, and budget, and responsibility and accountability.

So, I see a director of national intelligence who would have control over much if not all of the intelligence budget. He would not be the DCI. He would not be the national security advisor. It would not be the Secretary of Defense. It's the only way you're going to get accountability into the system, it seems to me. We do it that way for everything else in government; why don't we do it in the Intelligence Community?

Now what I've said has huge problems in terms of the practicalities of getting it put into place. I recognize that. But you asked me what I thought ought to be done. That's what I think ought to be done.

Mr. EVERETT. And I appreciate that. Mr. Webster.

Judge WEBSTER. This is one of the very few areas in which I find myself not entirely in agreement with Congressman Hamilton. I've been there. I've thought about the ability to function in both a detached DCI and a DCI that stays behind, and I'm not persuaded that that will create the kinds of synergetic improvements that you're looking for.

I would put more emphasis on finally addressing the lack of real authority that the DCI has over the Intelligence Community. He does not write the report cards on the agency heads. He does not even pick the agency heads. He has nominal authority over the budget, but I think it's really a matter of nominalist. In my years there we tried very hard and I got along pretty well with the agency heads, but we had to work at a consensus-building approach, even down to having our monthly luncheons at different agencies so that people wouldn't be concerned about DCI—rather CIA appropriating all of the work. But it had no real authority to make it happen. Occasionally I would issue something that looked nominally like an instruction, it was mostly hoping with a lot of groundwork behind it to hope that something would come of it.

If you're talking about the chairman of a think tank at the top rather than someone who can in effect give orders and have somebody do something about it, then I think it's another reason why I don't think that's the kind of leadership that's going to be required. So the British have some models. I don't really feel they fit our situation here, with all our checks and balances.

I would strengthen the DCI. I would not have a head of the national intelligence unless that national intelligence was actually running something. But if he's off at the White House with no troops, it's difficult for me to see how it would be truly effective.

I would look for ways to strengthen the role of the DCI in ways in which he does lead. Now, maybe that's going to mean someday that you're going to separate the two functions, but I don't know what you're going to give him to be effective in a room in the White House. I think you may be duplicating what goes on in the National Security Council.

Mr. EVERETT. Mr. Hitz.

Mr. HITZ. Congressman Everett, I find myself on the side of Judge Webster on this one, and I'm too young to be cynical; but having seen a number of these reports, what we're talking about, the 800-pound gorilla that the Director of Central Intelligence has always had trouble wrestling to the ground, of course, is the Secretary of Defense because of his authorities and responsibilities for the defense intelligence agencies. And I remember when the most recent report with congressional participation was produced several years ago under Harold Brown, who drafted it after Les Aspin died. At the end of the day, Harold Brown, himself a former Secretary of Defense, said that putting the SecDef under the DCI on intelligence matters was just one nut they couldn't swallow.

They recognized the need for the Secretary of Defense to have command authority, to support the fighting men, and they weren't going to give that up.

So maybe my opinion comes from too much time spent observing how this has played out in years past. But I tend to agree with Judge Webster that if you call a director of national intelligence the overall head and you give him some budget authority and no comprehensive operational responsibility—and I wonder how you could give him operational responsibility to control all the entities that are trying to gather and analyze information in this vast intelligence world—I think you may be following the illusion of some kind of reform and not getting the reality of it.

It seems to me that the Secretary of Defense and the defense agencies and the director of central intelligence—this enhancement of the Director's authorities that you last looked at in '97, giving him a kibitzing power over the selection of the Director of NSA and more collaborative powers with the Secretary of Defense, it may seem not a very dramatic resolution, but it may be the realistic one.

Mr. EVERETT. Well, this is interesting. We have different opinions there, and from people we respect very much.

Mr. Webster, you're in a unique position. You've been both the DCI and head of FBI, right? Yes. When you were DCI, did you find yourself in turf battles with the NSA and CIA, NRO and FBI?

Judge WEBSTER. Well, I tried to avoid that as much as possible.

Mr. EVERETT. I understand. But did you find yourself in some turf battles?

Judge WEBSTER. I would not define it as turf battle. I would define it as people sort of going their own way and not necessarily keeping you informed. There were issues. The one issue that was troubling to me was the correlation between the FBI and the CIA over counterintelligence. I established a counterintelligence center about 1988, after I went over to the DCI, and I filled it with seats from all of the principal agencies, including the FBI. But the FBI never assigned a permanent representative. I don't know what the

concern was, that we were engaging in turf encroachment on their responsibilities. They had people who would come and attending meetings, but no secundees. Later, after problems with Aldrich Ames and other problems with respect to counterintelligence, the problem was solved by placing an FBI agent in charge of the counterintelligence center, and that seemed to make—resolve all the turf differences. I just give that as an anecdotal approach to how you can deal with some of these things.

Defense is another issue because of the enormity, as Mr. Hitz pointed out, the enormity of their budget in relation to the total intelligence budget, and their special needs for isolated purposes, for their military purposes, and their reluctance to yield up any of that, much of NRO, the NSA, NIMA, a whole host of important intelligence agencies are under the Defense Department umbrella.

And I would anticipate considerable resistance if any of the Scowcroft recommendations, for example, were seriously considered. It needs to be talked out. I don't think it's life and death, but I do think that the suggestions that have been made don't address that particular problem.

Mr. EVERETT. Of course, we haven't seen that report yet.

Let me just mention—and I have great admiration for your experience, and mine has not been near what yours has been. I've been here 10 years, and four years in Investigation and Oversight Chairman on the VA, but I must tell you that the turf battles I've seen firsthand in this place have been tremendous. And I'm almost certain that we do have them in the community.

Judge WEBSTER. I'm sure that you do, but my experience over that whole period convinces me that it starts at the top, that the attitude of the leaders has a tremendous impact on the people who work in those organizations, starting with the problems between the DCI Dulles and J. Edgar Hoover and working their way through. If the people think it's not career-enhancing to work together, they won't work together.

We even had—I even went to the extent with Admiral Turner when he was DCI of publicly playing tennis together so that they would know that we got along and we hoped they would get along. And then there have been other things. I think that Director Tenet and Director Mueller have worked very hard during this crisis to demonstrate that that's what they want, is cooperation and working together.

Mr. EVERETT. I must agree with you that they have worked very hard in that direction.

General Odom, you wore the suit. But you were also the Director of NSA. Tell me about your relationship at NSA with the Secretary of Defense, and not a long thing. Was it a good relationship, and also, who did you feel that your boss was—the DCI or the Secretary of Defense?

General ODOM. I had a very good relationship with Cap Weinberger. Any time I wanted to see him, I could go in to see him. I always felt that I could do the same thing with Bill Casey and Bill Webster, who were the Directors of Central Intelligence at the time.

I just followed what were the legal definitions of the position. The DCI had two kinds of controls over me. He could really dictate

a lot about my budget. As I tried to make clear in my testimony, I don't think any DCI has been served very well by staff. Because of the way it's organized, he can't see how to effectively use that power as much as he could be if he had a program budgeting approach. He'd have a lot more leverage if he had that. And that's something to be done within the community.

The second point is, I depended on the DCI and what was produced from his staff as my collection guidance. I didn't decide to collect signals in South America because I particularly liked South America. You get it because the DCI has sent the national signals intelligence list out to you each year telling you where to put your money and where you wanted the intelligence to come from.

So I looked at Weinberger as my commander, but I looked at the DCI as my operational control. Now, in the military we have that. We have unified commanders in Europe and East Asia and other places. General Franks, for example, at CENTCOM, he doesn't command those forces in the sense of a solid line. He can't——

Mr. EVERETT. Let me interrupt you just a moment. What part does the budget play in operational command?

General ODOM. It doesn't play. You've got two things going on. I tried to make the point in my testimony that there's an operational management issue and there's a resource management issue. They're different worlds. In the Defense Department, the services do resource management; the CINCs do the operations. And you have that integrated, mixed up, not very well-clarified within the Intelligence Community.

Mr. EVERETT. And you wouldn't subscribe to the idea that whoever controls the budget controls the operational?

General ODOM. He who controls the—yeah, sure. I would agree with that in principle, yes. That's my point about—the DCI, I think, now, if he wants to, can have a big impact. He did in my day have a pretty big impact on what my budget was.

Mr. EVERETT. Eighty-five percent of the budget's over in Defense.

General ODOM. Right. But how the programs—they fenced that budget. And then my budget was scrubbed by the community staff. They would go through that in great detail. There were particular cases where I saw very big signals intelligence programs in the NRO that we really didn't need. I couldn't take that money and move it. Instead I just had to live with it.

Mr. EVERETT. Mr. Hamilton, would you talk about budget authority and how you see it and where it ought to be?

Mr. HAMILTON. If you don't have the budget, you can't get anything done. The person who controls the budget controls the operation. And if you don't have budget authority, you are dramatically undercut in your ability to manage the operation. That's why the bureaucrats fight so hard over budget. Budget is power.

Mr. EVERETT. And you would put that budget control under DCI? Or did I misunderstand you?

Mr. HAMILTON. I put it under a director of national intelligence. And that person would have real budget authority and real personnel authority. I wouldn't put him in the White House, as Judge Webster is suggesting. I think you've got to give him real authority.

Now, the criticism made of my position is that it's unrealistic; you just can't get it done. That may be valid. That may be valid.

But I wasn't approaching it that way. I was trying to think, through my testimony, how I would structure this in the best of all worlds, if you would. And that's the way you would do it.

I am impressed by the fact that after September 11, you have an altogether different national security environment and that an institution like the FBI, which has previously been focused on law enforcement, has now been told that its number one responsibility, its number one priority, is prevention. That means intelligence, because that's how you prevent.

We're in a new world, and we have to begin to think of ways to structure this. I have heard the argument about strengthening the DCI for 35 years. Let's strengthen the DCI; let's give him a little more authority, I'm not against that; I think it's been helpful. It's a move in the right direction. But I don't think it gets us into the new era we're in.

Mr. EVERETT. Then you would let the DCI control the CIA.

Mr. HAMILTON. The DCI would control the CIA. I don't think it's a good idea to—I think General Odom used the phrase "double-hat" in his testimony earlier—have the head of Central Intelligence be the head of all the intelligence. I don't think that works very well.

Mr. EVERETT. Thank you, gentleman. I apologize; the red light is on. We've spent an awful lot of time on this. As you said, it's been going on for a number of years. But unless we find out how to head this thing up, I don't know how we'll accomplish anything down the road. Thank you very much. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you very much, Congressman Everett.

Senator Rockefeller.

Senator ROCKEFELLER. Thank you, Mr. Chairman. I pray that out of these public hearings is going to come, yes, some more public understanding of what is and is not happening in the world of intelligence.

But more importantly, I hope that because they are public, the Intelligence Community is listening very closely, because there have been some things uncovered here which have not been a part of the public domain. And the whole question of the 85 percent of funding controlled by the Secretary of Defense and 15 percent by the Central Intelligence Agency Director is not known. There are huge problems like that.

What I fear and what I hope our Chairmen and our membership will not allow to happen is that this becomes another study without a report. We have very good reports, but there may be no action. I share your frustration.

Mr. Hamilton, I want to start with a "towards-us" question for you. When you're talking about reform in intelligence, you're also talking about decent, good oversight. And we do that, but we do it on a very short time line, because, unlike any other committee of the United States Congress in the House and the Senate, we are constrained by the number of years that we can be on this Committee.

I know a lot about health care. It took me 12 years to learn it. This is much, much, much, much more complicated. After eight years, I'm off. Chairman Graham, who is a superb chairman, has

to leave because the minority and majority have a rule that you can only do eight years and then you're off.

So you can't build up the expertise, I mean refined expertise. You can develop knowledge but you can't get the refined expertise that you need—the nuances, the countries that you've been to, digesting, ingesting, thinking through, rejecting bad concepts that appeared to you when you first kind of encountered them, and then you discovered they weren't as good because of other things. It's mature learning.

The reason they have that, I think, is because of power. So many people want on these committees. I don't know; I have no basis for saying that, but that's my judgment. And I think it's really damaging to the oversight, because I think it encourages "gotcha." It encourages, when people don't have adequate information or they don't have refined, matured information, what they do is they retreat to attack, because it's always easier to find something wrong with the other people than it is to figure out what should we do.

Eleanor Hill listed all these commissions. You say for 35 years you've been waiting. Well, there's a reason for that, I think, and part of the reason is that we are limited in our oversight and therefore not sufficiently confident in our oversight and don't have sufficient time for our oversight. And because of this, what I call ridiculous, eight-year rule, I would like your judgment, as a former chairman, on that matter.

Mr. HAMILTON. Well, I think you've stated it better than I can. I would remove the limits. I think it's six years in the House.

Senator ROCKEFELLER. I think it's now eight years.

Mr. HAMILTON. Eight years, is it? I'm out of date. So it's eight years. When the Intelligence Committee was originally put together in the House, the idea was to put on it very, very senior members who were inside players who would not speak to the press. Chairman Boland was chairman of the Intelligence Committee for a long time in the House. I don't recall exactly, but I don't think I ever recall an interview he gave to the press. And you did not want to have a big turnover.

But because of the pressure—as you said it's the most popular committee. Congresswoman Pelosi is here; she's part of the leadership. I know she would say, or at least I think she would say, that it's probably the most popular committee in the House, or among the most popular committees. So there's enormous pressure to get on the committee. And the six-year limit becomes a political judgment, in a sense.

From the standpoint of effective oversight, I agree with your comments. You'd be better off to have people who get intimately acquainted with a very complex subject matter. I think I was on the Intelligence Committee at least two years, and maybe three, before I understood the terminology. The field that General Odom worked in is enormously technical. And a fellow who comes out of Indiana and didn't know anything about those things had a hard time.

So I'd take the limits off. I know that creates problems for the leadership. But in terms of effective oversight, it's the best thing to do.

Senator ROCKEFELLER. I thank you. I won't ask others for their opinion.

If we invade Iraq, it would not be impossible that there would be retaliation. And if that's the case—and retaliation in the homeland—then that brings up the question of how ready are we, and what about all those sleeper cells, and what about the ones that will exponentially grow because of what will then follow? And who knows what follows upon what follows? That brings up the question which I think was discussed to some degree when I was coming back, and that is, if you've got this, Judge Webster, you say this refined sensibility about let's keep America the way America is, and I agree with that, but you have a situation where right now you have about, I think it is, 11 FBI people working in counterterrorism at the CIA, and about 25, including 19 analysts from the CIA, working at the FBI. It's not what I would call sort of covering the country.

Now, nobody wants to put the CIA in charge in terms of the intelligence-gathering in this country. I'm not sure I agree with that, but that's the deal. It would be very hard to do around here. So we talk about, well, we've got to get some alternative organizations, some alternative way of doing it, or we get a cabinet secretary or we get somebody who's in charge of the whole thing.

But in practical terms, as you said, Judge Webster, this whole deal has so changed, and this next 20 or 30 years is going to be so dangerous that we have to think in very, very different terms. And just as people don't like being strip-searched when they go through the airports but they get onto an airplane and they're safe, they adjust. If they want to travel, they do what's necessary. As you said, there's not enough security until you need it; then you can't get too much.

So to each of you, I would like to ask a question which may have been asked before. What do we do about that? And I'm going to predicate that with the inspector general report on the FBI that came out recently. The Department of Justice inspector general released this—that in spite of 9/11, as well as a commitment made three years prior to that—I'm looking at the FBI now—the FBI has yet to perform a comprehensive written assessment of the risk of the terrorist threat facing the United States. That's right here.

Number two, according to that same report, the FBI has not established a core training curriculum. And this is your point, General. There are two different people, two different cultures; one is not the other. But you think they'd be doing this sort of core curriculum training, if there was a chance of turning an FBI agent into an intelligence-gathering operator, that there would be training. There are no proficiency standards for incoming agents working on counterterrorism, nor does the FBI measure the proficiency of agents working on counterterrorism squads in the field or in headquarters units.

And he says that the type and extent of counterterrorism-related training varies throughout the FBI in a way which is not helpful; this, despite testimony the Committee received last week that the FBI in 1998 established counterterrorism as a tier-one priority.

Now, I just ask you—waiting 35 years, 9/11, we're either going to go to war or we're not going to go to war—but somebody has got to figure out where the bad guys are at home. And I want answers from each of you as to how that ought to be done, in your judg-

ment, without being too careful about what you say. I want answers that are helpful to this committee. Maybe they're answers that can't get passed in legislation; so be it. But what should happen? General.

General ODOM. I would repeat what I mentioned earlier. I think the counterterrorism function—and it would be both domestic and foreign counterintelligence; that is, focusing on gathering intelligence on intelligence, and I think it will overlap into terrorism very heavily—should be pulled out of the FBI and should create a new counterintelligence service.

Now you made the point earlier that we're going to have something happen here and who's going to watch for all these sleeper cells? Analysts can't do much about watching for sleeper cells. It's going to take a lot of people who are field agents looking at them, people who will commit themselves to surveillance time, to the activities that are required to run these kinds of operations. The weakness of U.S. counterintelligence across the board, in the military services and elsewhere, has been inadequate resources to do this kind of thing. It's not sexy compared to the intelligence of finding an enemy tank or an airplane or what somebody's political program is in a foreign country. And it's always been less well-funded.

I don't know how you can—if you mix the law enforcement—you've got plenty of law enforcement people out there to arrest people. But to surveil particular cases and to gather the intelligence which you can then turn over to law enforcement to bring them in, strikes me as another business. You have to separate that out. We will miss some. It's like other kinds of things. But we will increasingly become more proficient at it.

I would cite the experience of how Britain has dealt with Northern Ireland. They've had a member of the royal family killed. Part of it is learning to cope psychologically with the public at large. Now I think a hearing like this maybe can contribute to that. But I think we will learn how to cope. We'll become much more skillful in identifying those. But you won't unless we make this organizational change where the intelligence function here is separated from the law enforcement function.

Mr. HAMILTON. Well, I think the threat of terrorism is going to require an unprecedented overlap between intelligence and law enforcement. And we understand that both of the primary agencies here, the FBI and the CIA, have operated for a very long period of time doing what they have done, and I would argue they've done it quite well.

Now they're suddenly confronted with a new world, and the Director of the FBI is told and says, our number one priority is prevention. Now, that's a huge change for the FBI. It just turns the agency around from a law enforcement agency to prevention. And we cannot expect that to turn around on a dime. It's like the ocean liner. It takes a while to turn it around.

I have a lot of confidence in Director Mueller and in Director Tenet. I think they're very good people. I think they're very keenly aware of this problem, and I think they want to try to correct it. What does it require? It requires, then, first of all, leadership at the top. If you don't have the leadership there, you're not going to get anywhere. I don't think it's a statutory solution, a legislative

solution, to the kind of problems you cited a moment ago. A couple of them surprised me a great deal.

And may I say that, in this role, the oversight function that you perform becomes exceedingly important to see whether or not the FBI and the CIA, and other agencies perhaps, are doing the kind of job you want them to do. And it requires more and more tougher oversight, because they have been asked to go through such a remarkable transition in the focus of their agencies. And there are thousands of people that are involved here.

So it takes leadership, it takes oversight, and it demands, in that oversight process, that you insist on the sharing of information that is at the heart of so many of the problems.

Senator ROCKEFELLER. Chairman Hamilton, I hear what you're saying. The gentleman on your right made what I think is the ultimate statement: No organizational reform can overcome the absence of effective leadership and management, but dysfunctional organizational structures can neutralize the efforts of the best leaders. I think that's our problem. It's dysfunctional organization.

And I want this to go on to you, Judge Webster. You say it takes time. I don't know how much time we have. We probably don't have the time for that cultural change. We had a hearing the other day—I'll put this to Judge Webster—when we had an FBI agent from Minneapolis who had dealt some with the Moussaoui situation, and he had two alternatives before him. One is that Moussaoui's French visa had expired. That was a bad thing. He enforces the law and so he went that direction.

His alternative was that there was some evidence that Moussaoui might have terrorist connections. He chose to ignore that—not surveillance; that's not his job. I said, but how could you possibly pick the choice not to surveil over expiration of the French passport? Because basically that's my job.

Now, how do you, in fact, change that culture? We can talk about it. We can say it happens. The ship turns slowly. But it isn't going to happen, is it?

Judge WEBSTER. I don't know quite how to walk into that question.

Senator ROCKEFELLER. Try your best, sir. You've done it all.

Judge WEBSTER. First of all, one of the problems that worries me about too expansive a view of prevention is that the next word you hear is disruption, and that any technique to disrupt something is the thing that you want to do, even before you've run the surveillance that you were talking about to get the greater information. So it's stop this fellow quick, whoever it is; disrupt the organization.

I hope those things I heard right after 9/11 have been digested and refined and that we're not looking at that kind of a situation. It is one investigative tool when you have a bad guy. I mean, Al Capone went to jail on income-tax evasion. But the importance is not—it's not a cultural problem, that he didn't want to look into the terrorist thing. He believed he had something to stop the terrorist.

I don't know the full facts, but I can relate to why he did it. We had the same problem in drugs, learning to let drugs run under control so you could get to the top and find out what was going on

about it. Other countries even, you had to arrest somebody the minute you saw a drug on the table.

The FBI has developed a capability, and it needs a much stronger capability now, to work with the information coming from abroad, primarily through the Central Intelligence Agency, to mesh that information and follow up on those leads and to be sure that that information is delivered to the right people and acted upon.

We have to have that interface. As I tried to say earlier, counterterrorism is not pure intelligence. It's not about finding a throwweight of a new Russian weapon or looking into economic issues that might result in some adverse circumstance around the world. It's about crime, here and now, being planned against us. And we need to have people in place who can deal with it. If the numbers are wrong, the numbers can be quickly adjusted and should be.

I don't warm to the idea of separating counterterrorism from the FBI. We're not England. We're not 500 miles across our territory. We have thousands of miles to cover. Would you propose to create an organization that had people all over the United States, as the FBI does?

It does a remarkable job with its 11,000 agents, one-third the size of the police force of the City of New York, but I'd hate to think of what this new organization would have in the way of people in place, trained to anticipate, to pick up information on the spot, on the scene, in the United States, about unusual activity, to report it back and expect to have it acted upon. You wouldn't have that.

And I fear you would never vote the resources to have a second FBI throughout the country. So better to use what we have and train them to be more responsive, as you pointed out.

Senator ROCKEFELLER. Yes, okay. Mr. Hitz.

Mr. HITZ. Senator Rockefeller, just following up on that comment, it seems that in a number of these instances, the first responder is going to be the local police. It's going to be the local person who is checking trucks that go through the Lincoln Tunnel. It's going to be the person on the checking line at an airport.

And what you're going to—it seems to me what you do to amplify—the force multiplier here is going to be CIA and FBI and their responsibilities getting more proficient, but also interacting with people on the ground who are going to have the first contact.

Senator ROCKEFELLER. That's right, Mr. Hitz. And in West Virginia we have a superb state police which I governed for eight years, and they have 63 detachments. And as of about eight months ago, seven of them had Internet capacity. So, now, you tell me how they get this resolved.

Mr. HITZ. Well, they obviously are going to have to find some way to get some resources to do that.

Senator ROCKEFELLER. And so resources, resources, resources. I understand all of that. People don't come forward. They don't put their positions on the line. I'm chairman of the Veterans Committee. The first question I always ask the person who comes up before us for confirmation, at the beginning of a new presidency, is, if you don't get the budget that you need, will you go into the

Oval Office and put your job on the line and say, I'm going to get this? Will you bypass OMB?

OMB has to clear every single piece of testimony that's given before any committee in the Congress; OMB has to do it. That's Mitch Daniels running the President's OMB. Okay? And so I asked him that. Are you willing to put your job on the line? And that's where we get into the 85–15 thing. Defense has 85 percent of the intelligence budget. You know, George, who I think is terrific, has 15 percent. He isn't going to stray outside this 15 because he'll get knocked down by the Secretary of Defense every single time. And so the pattern continues while we talk.

Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Senator Rockefeller. Congressman Condit.

Mr. CONDIT. Thank you very much. Let me say to the panel that I'm delighted that you're here and you've been very informative with your testimony and your written testimony as well as the articles and commissions and various statements that you've made in terms of reforming the Intelligence Community.

And this is a totally serious question. It may sound like I'm being sarcastic, but I'm really not. I know that Congressman Hamilton has mentioned 35 years of work, and all of you have put in a decade of suggesting reforms. Can you tell me, do you have an idea why we can't reform the Intelligence Community? I mean, is what we're doing here today and what we've been doing the past few months, is this going to be helpful, in your opinion, to reform the Intelligence Community?

I'm not advocating one of your suggestions or plans over another one. I think they all have some merit, and you probably could pick and choose items out of each one that would be beneficial. But what's the reason we can't fix it, we can't change it, we can't reorganize it?

Mr. HAMILTON. Mr. Condit, I think, first of all, substantively it's just very difficult. You've got a vast enterprise. You have thousands and thousands of workers. You have dozens and dozens of agencies. And it's terribly difficult to develop a consensus on how you put these boxes together and to whom you give authority and take away authority.

It is one thing to be in favor of reform, but it's quite another thing to agree on how you reform. And we have never been able to build a consensus, because substantively people have very different opinions.

Secondly, the politics of it are very tough. It follows a little bit from the first point. But you begin to take away budget authority from the Defense Department anywhere and you run into formidable resistance. And I just pick on the Defense Department, which may not be fair, but it's probably true elsewhere as well. As you move boxes around, you're shaking up careers and changing pensions and health care systems and all the rest. It becomes very, very difficult.

I would not say it's we can't reform. We haven't succeeded at reform, because substantively we have not been able to get an agreement on a plan. You heard the differences of opinion expressed in this panel.

Mr. CONDIT. And I appreciate that.

Mr. HAMILTON. And, then, secondly it's very difficult to do because of the politics of it.

Mr. CONDIT. Well, whose responsibility is it to knock heads if we have to on that? You are talking about bureaucracies, you are talking about turf battles, you are talking about—but is it our responsibility, the Congress?

Mr. HAMILTON. I think the only way you really get major change in the organization of the federal government is from the President. The presidents really have to take the lead, otherwise you just can't get it done. The country was floundering around on Department of Homeland Security, all kinds of opinions out there. The President comes in and says, we are going to do it this way. That focuses everybody's attention. And he's the only person that can really move the bureaucracy in something of this sort.

For presidents this would not be an easy decision. It's a very, very difficult call for a president. Why did the President leave out of the Department of Homeland Security the FBI and the CIA? Well, I personally think his judgment was correct about that, but as a logical matter, as a rational matter, you would put them all into the Department of Homeland Security probably.

Mr. CONDIT. General, you want to make a comment?

General ODOM. I think the way to address that problem best is to ask who the users are. Intelligence is to be used. And if the users are happy with what's being supplied to them, then the organization is okay. If they are not happy, then they're the people who ought to try to change it. And I think that drives it back to Mr. Hamilton's point that the President—it has to start here. I have thought about this a lot. It seems to be the real constituency at the national level for intelligence is the President, the Secretary of Defense, the Secretary of State. If they want to change it, they can do it. They could do changes that I'm talking about, except for a national counterintelligence system, with an executive order.

The big users, the really big users of intelligence, are the military services—and you don't even have that in your budget here. And if you take sort of off-the-wall proposals like I heard the Scowcroft proposal, where you would move the signal intelligence and the imagery out of the Defense Department, you know exactly what will happen: they will build their own there, because when they are outside they will not serve the Defense Department.

I've had many experiences of calling up CIA and trying to get tactical support. They work for the President. They don't work for the Defense Department. I don't think you want to outsource your plans writer if were a military officer trying to run an operation. I don't think you'd want to outsource a lot of activities in that regard. And if you are going to put everything outside these departments under some other umbrella, then I think you have got a real problem of solving the support to the users.

As long as the users are happy with this, it is going to continue just like it is. Therefore I agree with Congressman Hamilton. I would say that I think you have an opportunity now to do something about the counterintelligence, which you haven't had before because the politics have just been impossible. I think you probably can do that piece. That's why I chose that. I think the DCI could

on his own separate these two positions and begin to act more like, and use the program authority.

I don't know whether we are talking on the same sheet of music or not with Mr. Hamilton here on controlling the budget, but there is a lot more power in control of the program than maybe you understand, unless you've been through it. Once it's programmed in there, we can't move it out of the law the way you allocate it without coming back reprogramming it, et cetera. And if the DCI staff really exercises effective control over that, you will have a lot of say. It has never done that effectively. One of the major reasons it hasn't done that effectively is this other structural issue. And that's the NRO arrangement—how it gets its money. And that's why I chose those three things.

If you want to have a major effect on opening up for more—better performance, it is the counterintelligence issue first of all, and second I think it is the DCI really becoming head of the community. And, third, it's creating this national program management system.

Mr. CONDIT. Moving along—and I appreciate that. I get it that you think there are some organizational changes that can be made without the President or the Congress acting. But I would think that we have to take some role in this. We can't sit here and point our finger at the bureaucracy and say they ought to do this and they ought to do that, without us—would you agree to that? Would——

General ODOM. I agree with that. I should have added the constituency that I think can change it includes not just the President, the Secretary of Defense and the Secretary of State, who is a very important user, but also the chairmen of the committees here. And it will be the Chairmen not only of the Intelligence Committees, but it will be of the Armed Services Committees—and probably, in the case of counterintelligence, the Judiciary Committee has oversight over the FBI.

Mr. CONDIT. Let me just think out of the box for a minute on Mr. Hamilton's suggestion on the DCI being the, I guess, overall authority for intelligence at the White House—is that right, Mr. Hamilton—and what Senator Rockefeller said about law enforcement and local agencies. How do you tie all those together? I mean, there are some countries who have centralized police, federal police. Are we talking that? I mean, because the problem is that, you know, we have communication problems with local law enforcement, the first responders, so on and so forth. Is that where we are headed? We have—

Judge WEBSTER. May I try to answer that question? If you are talking are we headed toward a federal police, I'd say absolutely not. I think if there's anything that's fundamental in this country it is that we do not want a federal police system, and that's why we have the checks and balances that are there.

We have to build up a more effective means of communicating between federal authorities and state and local in the times that we are going through. And rather than spending a lot of time on moving the boxes around, I would recommend that this committee and the Congress look to see those areas in the system which need badly to be shored up with appropriate resources and training—

and I'll give you one example, because I think it's crucial. There's a lot of talk about sharing of information, a lot of talk about gathering it and getting it to the right place in a timely way. And we have heard—I have been reading the reports of witnesses who've said where the failures have occurred. One place where the FBI has been trying to get help for years, and has not succeeded, is in its information structure, it's information case—automatic case system. It's gone from one extreme to the other. It has senormous amounts of data coming in, woefully inadequate means of mining that information, and other shortfalls in communicating it out to people who need to know it.

It's a 12-year-old system. I don't know a single successful business in this country that gets along on a 12-year-old system. They could only ask it limited numbers of questions. They can't do like I used to do as a navigator in World War II and the Korean War. I wanted as many fixes, lines to narrow the focus and get the information, not ask it a question like what is Alaska and get a room full of information, and that's all I can ask. It really needs attention. The TRILOGY, the three patchwork system on which a lot of money has been spent, is not adequate to the task ahead. If we are going to bring everybody into this picture, we need to know who needs it, who doesn't need it, what is it we are trying to find, and what do we have—and move it along, and to share that with the Central Intelligence Agency and vice versa. The DCI's whole purpose of gathering—they're much further along the line in knowing how to do this. They have the filing systems, the retrieval systems, and the dissemination systems that the FBI simply does not have, and badly, badly needs.

And I—if I just had that one—could impose on you to make that suggestion, look closely at the FBI's system for managing data, because it's worthless if it cannot reach the right people at the right time. And that's the kind of improvements that I think you can do. It used to be there was some cynical thing that the people in Congress would tell their constituents, they added a thousand new agents. And I was saying rather why not a new computer? And they said, There's not a lot of political value in a new computer.

But we have to put aside those, as I know this Committee is doing, and see what's really needed. Make sure that the FBI is fully equipped, not worry about how many more people, but worry about do they have the ability to match up in an appropriate way with the Central Intelligence Agency and the Intelligence Community—because that's what everyone is complaining about—things that went unnoticed or undetected or uncommunicated. And if you could help us in that area it would be a major step down the road, far better than——

Mr. CONDIT. Judge Webster, you lead me in—I'll get back to you, but he leads me into an area that I just want to touch on briefly, and it's a little different than what we talked about this morning.

And one of the principal findings I think of the Joint Inquiry so far that we have come up with is we have done a very poor job in sharing information within the Intelligence Community and between agencies and government that plays a role in combating terrorism. It's been pointed out—and you just did—that the new infor-

mation technology can be very helpful in linking us these groups together and sharing of information.

The concern I have is the technology can also be used vastly to improve our way of communicating with each other, but what about people's privacy and civil liberties? What suggestions do you have to how the government can proceed to take advantage of these tremendous capabilities without infringing upon people's privacies and civil liberties?

Do you have any suggestions for me about that, Judge Webster and Mr. Hitz as well?

Judge WEBSTER. I am certainly not minimizing privacy. I think my own shorthand quick solution—I know the time is running. The judiciary plays a major role here, and should in the future continue to do so. The fact that you have the ability to do something doesn't mean you should be allowed to do it, unless there is probable cause and meets our legal standards for doing so, getting the appropriate warrants. Even the problem we have now with electronic surveillance with digital privacy making it so difficult to do, you still need that warrant. But you also need help in making it possible. You get the warrant, and if you can't use it it is not much good to you. There's improvement that needs to be brought along the road.

When Abraham Lincoln was assassinated, 2,000 Americans were arrested, the entire cast of "My American Cousin." That's the way things were in those days. They didn't have fingerprints. They didn't have DNA. They didn't have other forensic capabilities. And they certainly didn't have wiretapping.

But the concept is with the emerging standards of decency, to which you refer, in our society—we just have to get better professionally. But I think the Congress's role is to be sure that we have the tools and that we are using them in accordance with the law. And that's an important role for the Department of Justice, and that's why I'd hate to see law enforcement go outside the Department of Justice at the federal level by giving it to people who are not trained and do not understand the requirements that the Constitution and our laws impose on them.

Mr. CONDIT. Mr. Hitz, I know you've made some comments in your testimony, but I would appreciate your comments as well on this.

Mr. HITZ. Thank you. Thank you, Congressman Condit. I just wanted to say and interject as far as what Judge Webster was saying about the needs of the FBI for help in the information technology, information retrieval and storage area, we wrote, oh, over a period of eight years, almost every management review, every audit we did of the Directorate of Operations records contained as a final recommendation. Could we secure money for the Directorate of Operations to modernize and improve its record system?

Because over a period of time, just as appears to have happened in the Bureau, monies were tight, and monies were obviously going to be used for operational purposes as opposed to meat and potatoes infrastructural purposes, if that choice had to be made. So I think there have been strides made in the CIA as a consequence of the attentions of this Committee and the pounding that we gave them from the inspector general's side. But it is an issue.

On the issue of civil liberties, if you will permit me an anecdote, yearly there's a seminar in Princeton, the Medina seminar, gathering state and federal judges for a couple of days to be lectured by or discuss with some of the faculty fine arts and everything else.

At the end of the session I had the privilege of addressing them on the subject of terrorism, and talked a little bit about civil liberties. Up a hand came from the back of the room, and a senior judge from Atlanta, whose name I never got, said, you know, I'm interested in what you say about not throwing the baby out with the bath water. I and four or five of my fellow judges contacted the Justice Department very shortly after September 11 to say that we had an awful lot of experience granting federal warrants in this area; we were willing to get on a plane, go anywhere, to help meet any crunch that the government may have to deal with the demands of law enforcement to move these cases along.

And I, like Judge Webster, would like to see a lot of the response to terrorism remain in the judiciary, remain in the Article III system, rather than being handled on an ad hoc basis. I think it can be done.

Mr. HAMILTON. Congressman, intelligence requires that the government get information, and information requires that you have to have surveillance on people. And some of those people may not be criminals. And so you have got a tremendous challenge here, it seems to me, to facilitate information-gathering from suspicious people who may not have committed a crime while trying to insulate legitimate personal and political activity from intrusive activity.

And the solution to it lies to a person like Judge Webster. When he was head of the FBI, he was extremely sensitive to civil rights and the rule of law. And that has to come from the top. You get a lot of hard chargers in the bureaucracy who may not have that sensitivity. You have to have that sensitivity at the top. And I think that's required. You have to do it in the courts—obviously that's the bulwark of our liberties, the courts. But I would say your protection here—and I really appreciate your question, because I think it's very easy to overlook these matters of privacy and civil rights—it has to come from the top of the agency. It has to be protected by the courts. The United States Congress, the intelligence committees, have to be sensitive to the manner in which intelligence activities are carried out, and they have to zero in on civil rights and liberties.

Mr. CONDIT. General, did you——

General ODOM. I would just add one point on the protection of rights. The committees that did the investigation in the 1970s did a great service in implementing the system they have in the National Security Agency now ensuring that rights are not violated. So we look back and say nothing was achieved by any of these committees. It just occurred to me that this was—this one was very important, and you are not getting any credit for it. I think Congress should get credit for that. And as the director of the agency I felt better for having this. I felt that I could be certain that my bureaucracy was not going to run away and violate these kind of rights. And it was a thoughtfully done process that created that system in the 1970s.

Mr. CONDIT. Thank you, gentlemen. Thank you for your answers, and thank you for your service to the country. I appreciate it. Thank you.

Chairman GOSS [presiding]. Thank you, Mr. Condit. We are at a convenient place to break for a luncheon recess. And the intent of Chairman Graham is that we reconvene at 2:00, and at that time we will have Senator DeWine asking questions for about 20 minutes, and then such Members as are here we will provide the opportunity to ask further questions, if that is agreeable to you all.

Thank you very much. We'll see you then. And we have had a very useful morning.

[Whereupon, at 1:07 p.m., the Committees recessed, to reconvene at 2:00 p.m. the same day.]

AFTERNOON SESSION

Chairman GRAHAM. I call the Joint Inquiry to order.

Our final designated questioner is Senator DeWine. Senator DeWine.

Senator DEWINE. Thank you, Mr. Chairman.

Let me just thank our chairmen for holding this hearing. I think, Mr. Chairman, we are now into the area that we should be into, and that is the future. We have a very distinguished panel, and I appreciate our witnesses staying with us this afternoon.

Chairman GRAHAM. Senator DeWine, I apologize. I should have made note of this. Judge Webster had a commitment that required him to leave after this morning's session. He regrets that he's not going to be with us. If there are questions that you would like to submit to Judge Webster for subsequent follow-up, I am certain—

Senator DEWINE. You just threw away a third of my questions, Mr. Chairman. [Laughter.]

Thank you very much.

Congressman Hamilton, I think one of the things that's going to come out of this Joint Inquiry is the understanding that Congress, and specifically the Intelligence Committees, have some responsibility for any of the intelligence failures that did in fact occur leading up to September 11. I think that's going to be part of it. We're going to talk about that, I hope, in the report.

You have really a unique perspective. You served for a number of years on the House Intelligence Committee. You chaired the Committee, chaired the Iran-Contra Committee. Now you've had a few years to reflect—I wouldn't say sit back and reflect but reflect—on this and continue to study it. What recommendations do you have for the House Intelligence Committee and the Senate Intelligence Committee and Congress in regard to oversight, in regard to structure, in regard to how we can better do our job?

How do we, for example, when we are dealing with agencies that have very closely-guarded information, understandably, how do we even know the questions to ask them? How do we exercise our Constitutional responsibility in this very, very important area?

Mr. HAMILTON. Senator DeWine, you are right. There is no independent oversight of the Intelligence Community except the Congress, and therefore I think the Congress has an additional responsibility. All Congressional committees have some oversight responsibilities. Here I think it weighs especially heavily. And because

the Intelligence Community is such a technical business, it's not easy for a Member of Congress to come onto an intelligence committee and understand the Intelligence Community.

The first thing I would say to you is that you should approach your job with a lot of skepticism. I don't mean that to be negative. I just mean you have to be willing to be critical of testimony and of propositions that are put to you. You have to be a partner and a critic at the same time. Your job is to try to improve the Intelligence Community, but your job also is to be very critical and to do it as positively and constructively as you can and not to be overwhelmed by the Intelligence Community. It took me a long time to get acquainted with the terminology and to be comfortable with the budget. And I think the key requirement is for individual Members to be skeptical.

I think, secondly, you have to hire a very good staff, and that staff has to have technical capabilities that you may not possess, or I certainly did not possess as a member of the Committee, because you are dealing with people who are testifying, like General Odom often did, on very technical matters. And you have to put in a lot of hours at it and take it as one of your number one priorities.

I don't have any magic solution for you. With regard to structure—and may I say overall that I think the Congressional Intelligence Committees, both Senate and House, over a period of years have done a very good job. They have been fortunate to have very good leaders. You have two good leaders here today, Senator Graham and Congressman Goss.

Senator DEWINE. We certainly do.

Mr. HAMILTON. And, looking back, I think I know the House situation a little better than the Senate, but I think the House chairmen—I hope Mr. Goss would agree with me here—have been quite good. So that's key.

The staff director plays the heaviest burden in making the Committee function well, after the two chairmen, and they have to be highly-qualified and very, very good.

I told Senator Rockefeller a moment ago that I think I would remove the term limits on the positions. Maybe a compromise position would be to extend them, but eight years I think is too short a time, because it takes you so long to get into it and to know where the problems are in the community.

Senator DEWINE. Do either of our panelists want to comment?

Mr. HITZ. I would. I'd like to do it perhaps from what you would regard as a parochial perspective, having been the Inspector General at CIA. Let me say that the support of this Committee, you after all created that office—you had to fight hard to create it—the support of this Committee on the work of an inspector general is absolutely critical. If you were not attentive to our product, our reports, whether you agreed with them or not, if you were not alert to the issues that we were trying to set forward, put a light on, just as the Director of Central Intelligence, to whom each inspector general reports initially, must do so, then that process insofar as it helps you with your oversight responsibility would wither.

And I can guarantee you that no inspector general doing his job in Washington can get along without an oversight committee that

encourages, helps with staffing, reads the product, follows up on some of the matters that are appropriate for them to follow up on.

I hope and I'm sure you're doing that.

Mr. HAMILTON. Senator DeWine, one of the things I was always worried about was that we were spending too much time on covert actions. There's something kind of interesting and catchy about covert actions and they are very important, but when I was on the Committee we spent an enormous time reviewing covert actions.

They are clearly important, but it can distort your vision a little bit and you don't put enough emphasis on collection and analysis, the quality of intelligence.

Senator DEWINE. Do you think that might also be a historical legacy of concern of Congress missing something?

Mr. HAMILTON. Yes, I think so.

Senator DEWINE. Paranoia or just concern, one or the other. It's an interesting point.

General.

General ODOM. I looked at the committees, after I became accustomed to the system, the way I think a college president would look at a college board. You were the source of my money and you had an oversight. You couldn't hire and fire me. I guess you could impeach me. But the Secretary of Defense and the DCI could do that. But this was not original with me. I was discussing this once with the provost at Boston University under John Silbert, and after we talked about college boards—I was on one at the time and we were talking about what you expect your board to do—and I found that model very insightful.

It fits very much with what Congressman Hamilton said about you need to be critical but you have to be supportive. And it has to be a symbiotic relationship. I mean, you'd like to have it there.

Senator DEWINE. Thank you. Let me move to a question that you were dealing with this morning, and I don't want to belabor the point but I think it is very important and I want to delve into it a little further, and that has to do with the role of the DCI.

I found it interesting that all four witnesses, if I'm summarizing correctly—and correct me if I'm wrong—seemed to believe that the DCI should have more power, but we break down there on any kind of consensus. It seems that if we have people who were very knowledgeable in this area from different backgrounds and if you at this point in your careers cannot reach any consensus, maybe this gives us a good indication of why we have a hard time making any change here.

But let me start first, though, with Congressman Hamilton. You talk about a director of national intelligence. If our goal, which it certainly is my goal, if our goal is to make that person stronger, how do we do that while at the same time removing any direct command authority he has or any direct authority he has to run a department? What stops him from becoming a drug czar? Now we have an intelligence czar, with all the problems that are connected with that.

Maybe all I need for you to do is just expand a little bit on it.

Mr. HAMILTON. Senator DeWine, it's just a very tough, difficult problem. I don't want to suggest that my thoughts are carved in granite on it. I think you have to have someone who oversees the

entire intelligence operation, and that means the direct answer to your question is they have to have budget authority, and if they have budget authority then they're going to be able to get a lot of things done.

Senator DEWINE. And you believe in the cabinet, a member of the cabinet.

Mr. HAMILTON. Well, I said cabinet-level. I would think it's a terribly important position. Really the key in all of this, whether you're talking about strengthening the DCI or having a DNI, is the relationship of that person to the President, because power flows from the President. And if that relationship is good, as it has often been in the past, it works pretty well. And then on several occasions all of us can remember it was not a good, close, candid relationship and it didn't work well. So no matter what kind of a structure you have, as is so often the case in organization, it depends on the personalities.

But this dual-hat role that General Odom referred to earlier in his testimony, I just don't think it works very well. You cannot be head of the Intelligence Community and head of the CIA at the same time. There's a conflict there. And I want someone over all of that.

And I must say my thinking is in part guided by the whole sense of accountability. The Intelligence Community is too mushy. You can't find who's responsible, and you need to be able to call one person on the carpet and say, by golly, you're the guy in charge and you perform or not. We have enough trouble with accountability in our government without having the whole exercise run by an Intelligence Community, I think.

So I would give them not only power over the budget; I would give them power to manage too.

Senator DEWINE. As you mentioned, we talked about this morning, and as I think Mr. Hitz said, the problem of getting this done politically we all know, and that is that you have the 800–pound gorilla of the SecDef and other problems, and unless——

Mr. HAMILTON. But if you take that budget authority out of DOD or these various systems and put it under the director of national intelligence, it's going to make a whale of a difference as to how the place is run.

I don't want to denigrate the military intelligence, but military intelligence is very important but it's not the whole world of intelligence. There are a lot of things we need intelligence on other than the military. And when four-fifths of the budget, or whatever the percentage is, is run by the military, the Defense Department, that means a lot of other things are going to be neglected while you're providing military intelligence. Military intelligence is important, but it's not the whole world.

You need people who can tell you whether India is going to produce a nuclear weapon or not, or whether the Soviet Union is going to collapse. And those are not strictly military questions.

Senator DEWINE. General.

General ODOM. I'd like to comment on this.

Senator DEWINE. Sure.

General ODOM. NSA supplies information to probably more agencies than any other intelligence organization, so it has a big cus-

tomer base. Only one of those is the Defense Department. The Defense Department is only one of those. At least two-thirds of the people who are collecting SIGINT are in uniform.

Senator DEWINE. General, let me just interrupt you, though. Isn't it true that the budget, though, is controlled through Defense? We've had example of the defense budget. My only point is whoever controls the money controls the priorities, and when it comes down to crunch time—and we've seen in this Committee, sometimes behind closed doors, examples of where the priorities get worked out, but——

General ODOM. May I finish this point?

Senator DEWINE. Sure.

General ODOM. I was going to point out that you have a huge amount of defense money providing massive intelligence to the civilian users. The problem I had at NSA was that the military was upset that they were working for non-military people most of the time. And the biggest part of NSA's customer base, except in really wartime or particularly against the Soviet Union a lot of it went to the military, but the bulk of NSA's output was being used by other people.

I mean, the whole drug business, Director Casey used to say you're producing 80 percent of the intelligence that supports the drug war. And we were producing it with soldiers and sailors and airmen. So I think when you try to draw those lines that's where the practical business, I think you can have a lot of authority with program management.

Once the Secretary of Defense sets, fences the money for the National Foreign Intelligence Program, then the DCI has unrestricted authority to move it around within that fence, even if it's defense money.

Senator DEWINE. Let me just move on. I apologize, but my time is running out.

Mr. Hitz, on October 21, 2001, in the Washington Post you said: The time has come to take off the gloves, to loosen inappropriate restraints and, even more importantly, to acquire the skills to understand and penetrate bin Ladin's circle.

Take off the gloves—you've got about 60 seconds.

Mr. HITZ. Okay. Again, all of this——

Senator DEWINE. Anything that we haven't done in the last year? That was a year ago.

Mr. HITZ. All of this is well familiar to this Committee. My view of it is that all of the approvals that were necessary to deal with controversial agents who had disreputable backgrounds have been streamlined. I'm all—I think there should continue to be the kind of good oversight from the standpoint of the chain of command. I'm not sure that each of these cases has to go to the Director of Central Intelligence, when you are thinking about picking up a felon as an advisor.

But let me just make my final pitch for the kind of training in area studies and in languages that all of us know are critical. And if you're looking at it from the standpoint of a teaching institution, if you can't get people to study the Arabic language, do what we did in the old days, the old-fashioned way—bribe them. We had a National Defense Education Act once that made monies available

to students to study hard languages if they were willing to commit their services to the government for a period afterwards. That lapsed with the passage of time——

Senator DEWINE. That's an excellent idea.

Mr. HITZ [continuing]. But it may be one way to deal with it.

Senator DEWINE. Let me ask any of the panel members this question. We've heard testimony recently from Secretary Armitage and Secretary Wolfowitz that both of them believe that one of the biggest problems with our intelligence and analysis is that the agencies strive for consensus and don't always encourage dissemination of dissonant views.

I wonder if you agree or disagree with that.

Mr. HAMILTON. I agree with it. I think there's tremendous pressure on the analysts to reach a consensus. The broader the consensus, the more general and sweeping the conclusion is, the less valuable it is. I think you want to encourage competition among your analysts and have majority and minority reports. If I were the President of the United States, I'd want some sense of the bureaucratic view, both for and against a given course of action.

I want competition among analysts. I think the minority needs to be protected. I think they need to be encouraged to speak up.

Senator DEWINE. Anybody else want to comment?

General ODOM. I would briefly say I would strongly encourage Members to go try to find a situation, look at it directly, where intelligence is used to make decisions. You are exactly right about reaching a consensus on the national intelligence estimates, the national documents that are produced by the National Intelligence Council. Even within some agencies like DIA, et cetera, there are consensus kinds of problems.

It's been my experience that almost no decision is made on that kind of intelligence. I'm looking for somebody to show me how an NIE caused a policy to change. The major advantage of an NIE is it makes the Intelligence Community share its information base. If we're talking about a problem of sharing for counterterrorism, that's with the FBI and people outside. We have made great progress in getting a common intelligence information base in the community.

If you go where decisions are made, you will find the user deeply involved in the intelligence process himself. To give you an example. When we were building the M–1 tank in the Army, the thickness of the frontal glaces of a T–80 tank was very important. Ten millimeters of difference would have changed it from a 120 gun to a 105 gun. It was very easy. I had the responsibility of deciding which way to go on that, and I was a big 105 gun fan, but I finally said okay, I'm going to do this way. That pushed about $18 billion around, to up the gun to 120.

Now that's where intelligence really plays. I never understood the big brouhaha of not predicting the end of the Soviet Union. It doesn't make any difference. Tell me what we would have done differently had we known it was going to end. Or, the issue of how much the Soviets are spending on defense. Nobody cared. It was a political game the CIA and the rest of the Intelligence Community played for the press. We didn't spend our money to buy based on

how many rubles or dollars they spent. I wanted to know—my army wanted to know how many tanks we had to kill.

So what we should be tested against is whether we counted the number of tanks and knew what it took to kill them. And that's where intelligence plays. And I'd go to the State Department and find where intelligence really helps them in their negotiations. And that's the test. It's not whether there's competitive analysis or these other kinds of thing.

So I have a kind of practical, hands-on view. If you want an answer to that that's clear, you're going to have to go and absolutely look and make people show you the causal linkage.

Senator DEWINE. Good. Well, let me thank all three of you. I appreciate your testimony. I think it's been very helpful for our Committee. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Senator. I want to thank the panel, but I also want to thank our four lead questioners today. I think they have raised very fundamental issues in a way that will be very helpful to us as we move towards our final recommendations.

We are now going to move into the five-minute questioning period, and I have the good fortune of being the first of those. I'd like to turn in my first five minutes to issues of personnel. My own experience has been that you can have the best organizational chart, but if you don't have the people who can make the system work you're not likely to be very successful. Parenthetically, I hope Steve Spurrier is not in that position.

Mr. Hitz, you talked about a number of things that might be done to enhance the personnel within the intelligence agencies, starting with the idea of more internships to introduce young people. There have been a series of other suggestions made which I'd just like to mention for purposes of stimulating your brief comments on those and then adding to your list of ideas.

There was a proposal in an issue of Foreign Affairs earlier this year of setting up an intelligence reserve corps somewhat analogous to the military reserves, which could be activated at a time of particular need, a proposal for an intelligence reserve officer training corps. Maybe that comes close to your suggestion that you just made about restoring the scholarships, the defense scholarships that used to be made.

Also, the issue in terms of getting more people in intelligence who can speak the languages and understand the cultures of the diverse areas of the world in which we're now trying to operate, that we ought to have a more aggressive recruitment policy towards non-traditional CIA and other intelligence agencies, specifically among the Arab-American population.

Could you comment on those and any other suggestions to improve the personnel quality? Let me just mention one other that I heard on a recent visit to our station in Cairo. That was that, almost like in the public schools, the agent's compensation is heavily affected by their years in service, and once they reach a certain level it's hard to show much more advancement, and at that point agents are tempted to leave their case responsibilities and move into an administrative position where they have more economic up-

side, just as teachers tend to leave the classroom and go into administration for the same reason.

Is there some way that we ought to be re-looking at the compensation strategy for intelligence agencies to keep our best people doing what they're best at and being rewarded for that superior service?

Mr. HITZ. There are a lot of good points that you've made, Mr. Chairman, and also ways in which I think aspects of them have been tried in the past but not pushed enough. I think the intelligence reserve corps has been attempted after a fashion, and I think you would agree with me, sir, that presently, with deficiencies in a number of language skills and experience levels, a lot of old boys have been brought back. They are in effect an intelligence reserve corps right now. They've gotten recent retirees to agree to come back and put their shoulder to the wheel after 9/11. That's an informal way of getting at that, but it certainly makes some sense.

On the question of trying to recruit operatives from America's Arab-American community to go back to the Middle East, I thought there was a very thoughtful unsigned editorial in the Washington Times a day or so ago making the point that that's not necessarily the answer to a problem, because natives of that region want to be dealt with by a real American, so to speak. I'm putting that in quotation marks. They want somebody that may not speak the language with absolute proficiency but is good enough.

And a perfect example of that is the Popov case in the cold war era, when the Agency sent a recent emigre from the Soviet Union to first deal with Popov when he was coming over to us from Vienna, and Popov didn't trust him. He knew what Stalin was able to do with emigres and wouldn't fiddle with it. So I think there has to be a sort of a balance on that part.

On the management side, as opposed to why promote a person who is a first-rate case officer into management and lose those talents, again that's a debate that's gone on long in the Intelligence Community and lots of people frankly, as case officers, don't want to be and aren't very good as managers. I think George Kiesevalter—I don't think I'm taking his name in vain—always considered himself to be a case officer till the day he died, even though he was a very senior intelligence officer.

But I want to be clear on the point. I don't think all of the talent for doing this work is going to come out necessarily of our finest universities. There are all kinds of skills that work in this area and, if I can be permitted just a personal anecdote to finish up with, my first boss in the Agency was a Nisei. He was a person who lived long enough ago in Los Angeles to be able to dive for abalone in Los Angeles Harbor. It's been a long time since that happened.

Well, he was sent to camp. His family were interned, and in 1942 the U.S. Army came along and recruited him to the counterintelligence corps. He served in Japan until the end of the war, joined CIA, for 30 years practicing his trade all over the world—an extraordinary person. Why there was no lingering bitterness, I have no idea. But he was absolutely first-rate. So this country has got an awfully broad range of talents out there to draw from.

Chairman GRAHAM. Thank you, Mr. Hitz. I'm sorry my time has expired, but when I rotate back I'd like to ask Mr. Hamilton and General Odom for their comments on the issue of personnel.

Senator Shelby.

Vice Chairman SHELBY. Thank you. There's been a lot of debate recently in the Senate about the creation of the Department of Homeland Security that you are all familiar with. Perhaps the most important part, at least I think so, of the Homeland Security legislation that's being debated is its provisions dealing with information analysis. Senator Graham and I have been involved, with Senator Lieberman and others, dealing with that particular piece.

If homeland security analysts are to occupy, if they are to occupy a unique position and have a unique perspective in that they would have access both, General, to domestic and foreign intelligence, and to information on homeland vulnerabilities, it seems that it would be important to give them the capability for this sort of deep information access to intelligence agencies, in other words, if they needed it or thought they needed it.

What are your thoughts here regarding the role of homeland security in the Intelligence Community and should it have an analytical component? And, without an analytical component, what would it be?

General.

General ODOM. It needs an analytic component. It doesn't just need one; it needs many. It needs a central one and then it will need distributed ones. Let me offer the model of mainframe central processing versus distributed processing in computers. When you had one big mainframe computer, with slow computers, dumb terminals, people got backed up in a queue. When we came to microprocessors, we could have a lot of people processing simultaneously.

Intelligence analysis is done the same way, and many users need analysis and you'd like to have the analysis with them. The collection can be more centralized. When you have the organization, homeland security, deciding where it wants those, I think it should have them near decisionmaking points, then each of those analytic capabilities need to be able to tap into NSA, the national imagery agency, to CIA's clandestine service, and to what I would see as the national counterintelligence service. The FBI will never give information out. A national counterintelligence organization would be an intelligence organization, not an arrest organization. Therefore they would have an incentive. They want their stuff used. They're not doing it for themsevles.

There's no reason that that analytic center can't draw on the whole community. The model that I think it's easy to look at right now in that regard is how the State Department works. You have INR at State, which is the general central point, but within negotiation you can have an analytic center supporting anything that's going on.

That seems to me to be sort of a straightforward, easy organizational issue to deal with.

Vice Chairman SHELBY. I agree with you, General. Congressman Hamilton?

Mr. HAMILTON. Senator Shelby, I don't know that I understand all that well the President's proposal on the Department of Home-

land Security with regard to intelligence. As I understand it, the Department of Homeland Security would not be a collecting agency at all. They would not get the raw data. They would get the conclusions from the CIA and the FBI.

Vice Chairman SHELBY. The whole community.

Mr. HAMILTON. The whole community, and then they would use that to assess threats and for the primary purpose of protecting the infrastructure. And the President's talked about it being a clearinghouse, and I think George Tenet has said the Department would be a consumer of intelligence.

I'm a little skeptical of all of that. I don't think the conclusions of the Intelligence Community, if handed to the Department of Homeland Security, will satisfy the Department of Homeland Security folks. They're going to want to know, well, where did this come from and how sure are you of this information.

Vice Chairman SHELBY. They're going to vet it, in other words.

Mr. HAMILTON. I think that's correct.

Vice Chairman SHELBY. And I think they should.

Mr. HAMILTON. You were mentioning they have to have some capability to examine information analysis. I think I agree with that. Now, if you do that, then what is the relationship between these three organizations—DHS and CIA and FBI? I'm not sure I know the answer to all of that, but I am a little skeptical of this idea that the raw data would not be available.

I also understand that the President would have the authority to provide the raw data, under certain circumstances, and that might work satisfactorily, but I'm reasonably sure if I were running the Department of Homeland Security and I got the conclusions from the intelligence agencies—those conclusions tend to be fairly broad and sweeping and vague at times—that I wouldn't be satisfied with it.

So I sense the Senate is quite correct in looking at this pretty carefully.

Vice Chairman SHELBY. I agree with you, Senator Graham and I. That was not the President's first proposal but we've worked out a proposal now.

My time is up. Can Mr. Hitz say anything, Mr. Chairman?

Mr. HITZ. Well, I find myself in agreement with Congressman Hamilton on that, and the only question I was going to put to you, Senator Shelby, was what is the recourse of the homeland security analyst if he finds that the intelligence he's provided is not up to snuff? This is the point. Does he have to go back to the President and knock on his door to get it right.

Vice Chairman SHELBY. He should be able to go right back and task someone what is this, what does this mean and so forth. That's what Senator Graham and I have been proposing for six months, I guess it is.

Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Senator. The next questioners, in order, will be Congressman Roemer, Senator Roberts, Senator Feinstein. That will complete the first round. Congressman Roemer.

Mr. ROEMER. Thank you, Mr. Chairman. I want to welcome all three of you here today. You have really been extremely helpful to

us in helping us look forward and help us try to come up with some answers to some of these very vexing and complicated problems. Congressman Hamilton, I want to especially welcome you before the Committee as both a colleague from Indiana and a good personal friend. We welcome your very extensive testimony.

I want to quote back from a line in your testimony which I think is extremely important to us today with the current threat that we have in the world and as we may be going into Iraq to do something about weapons of mass destruction. The quote is: If we were starting all over again I cannot imagine we would create such a vast enterprise and have no one clearly in charge.

We still have that system out there today. What do you think specifically we can do about this problem? And how big a problem is it?

Mr. HAMILTON. I think it's a very large problem. I think you have two basic options. The one option is to try to strengthen the DCI. I certainly don't oppose that effort because I think that needs to be done. I also think it's a very incrementalist approach that we have been trying for many years and we've never been really satisfied with the results we've gotten.

The other option is to go to a director of national intelligence that I have been arguing for. Obviously there are some problems with that as well. But those are the two options and I think you have to make a choice between them.

I favor the director of national intelligence. The criticism that Judge Webster and others have made is that it may not—and I think Fred as well—is that it may not be realistic. There's something to that criticism. I mean, I understand it's a very tough thing to achieve.

Mr. ROEMER. Congressman, you were just——

Mr. HAMILTON. But, Mr. Roemer, may I just say that we're in a new period and we've simply got to think anew here.

Mr. ROEMER. I couldn't agree with you more.

Mr. HAMILTON. And we've got to put aside the way we've always done business, and the way we've always done business is, if we give a little extra power to the DCI things are going to be okay. It's not going to be okay.

Mr. ROEMER. You were just talking about the creation of a homeland security department, where we all would probably have our complaints or criticisms about this part of that part, but it's an attempt by the Administration to centralize power and agencies, disparate agencies, under one roof. That's what you're suggesting here as well.

Mr. HAMILTON. That's correct. I'm looking for a way to improve, I guess, visibility and accountability in the Intelligence Community. I've gotten to the place where the very phrase "Intelligence Community" I dislike, because it's too vague. And one of the great problems in government always is accountability and getting someone to take responsibility, and I'm looking for that.

But I really think the quality of your intelligence will improve if you have a single person over all aspects of the Intelligence Community with responsibility for budgeting and personnel. I'm going to comment on Senator Graham's business on personnel in a moment.

Mr. ROEMER. Again for Congressman Hamilton, with respect to the need for creation of an independent commission, how do you feel about that?

Mr. HAMILTON. I favor it. I think that I come from the point of view that we need more, not less, oversight of the Intelligence Community that is independent of the Executive branch. And I think this Committee has performed a very important service in the last few months and weeks, but I don't think you've finished the job. I think there's a lot more to be done.

It's terribly important how we go about this. We ought not to be saying I'm looking for somebody to blame. We ought to be looking ahead and saying what were the problems in the system that brought about the shortcomings and how can we correct them.

Now you and I know that there are a lot of commissions in this town, some good, some bad, some indifferent. So it makes all the difference who you put on the commission. And I think there are a lot of good Republicans and I think there are a lot of good Democrats who can serve effectively on this commission and do the country well, a great service.

I don't worry about a little redundancy here or a little overlap. Indeed, I think it's probably good because it's hard to get this town to move on anything and you need a lot of people looking at any given problem. I know you've been a primary supporter of this in the House. I applaud that effort. I also understand the hesitation of the Bush Administration and maybe some of you here about this. You'll say well, this is going to be used to hang us or point out people who made big mistakes. I don't see it that way at all.

But we do have to be sensitive to that concern, I believe. But I think a real service can be rendered by further oversight by you, by the Committees, but also an independent commission as well.

Mr. ROEMER. Thank you, Mr. Chairman. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you very much, Mr. Roemer.

Senator Roberts.

Senator ROBERTS. Yes, thank you, Mr. Chairman. I also wish to echo the comments of positive advice and counsel from the four wise men. And, Lee, I would refer your speech to my colleagues. I got to Tab 9. While listening intently to every word that you said, I discovered Tab 9, which includes your speech of July 18, 2001, so you were just as prescient as usual in regards to when you addressed a hearing before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations—that's a mouthful—of the House Committee on Government Reform. So we thank you for your insight.

I just have a couple of observations, and if any of you three want to make any comments, I'd appreciate it. Number one, Senator Shelby asked my question in regards to homeland security and some kind of an analytical center. I just had the dubious privilege of being the President of the United States on Monday in an exercise called Crimson Skies—very similar to the Dark Winter exercise on an attack from Iraq—which makes you scratch your head a little bit today—on a smallpox inclusion and what happened as a result of that. It was a very helpful exercise. It has helped us

from the CDC standpoint of having vaccines now for every American in regards to a possible smallpox attack.

This was an agriterrorism attack, and the USDA was the lead agency. But it became obvious that there were a great many other agencies, more especially the Homeland Security Agency, which allegedly is supposed to take charge, and the Justice Department and FBI and CIA. And in the inclusion of things that happened to us we pretty much found out that after the incubation period you had about two or three days to make some decisions and it was already too late. So you had to make a lot of decisions prior to that. I think a lot of other agencies that took part in this exercise learned a great deal about the possibility of endangering our food supply which has now come into the top ten of things we worry about.

But we had the topoff exercises. And I'm wondering. Basically in terms of cooperation and information-sharing the joint investigative staff had an excellent summary of that just a hearing or two ago. If that's not the best way to do this in regards to forcing people to take a look at a problem or a challenge they had not really predicted, and then do an exercise and if you do the exercise obviously you are forced to make these decisions and then you get into lessons learned even with the first responders. That's one thing.

In regard to the second question, it is in regard to Senate Resolution 400. One of the things that I have discovered is that when we held a hearing over a year ago—Senator Shelby and others were very active in that, the Intelligence Committee, the Armed Services Committee and the appropriators of the Senate—we had 46 federal agencies come up. We asked them what their mission was, what they really did, and then who was in charge. Today there are 80 federal agencies; at that time there were 14 subcommittees and committees in the Senate alone who said they had jurisdiction. Now there's 88.

Obviously we have been selected as the Committee in regards to the investigation that we're doing now, and I know that Senator DeWine and Senator Rockefeller indicated that perhaps this select committee should be made a permanent committee. I'm wondering, with 37 members, if it couldn't be reduced, if it couldn't have a joint permanent committee between the House and Senate. It doesn't seem to me to make too much sense today to have them both in the House and Senate. And then basically limit the number of committees that Members could serve on, given the challenge we face today. Now that's not going to be very popular, more especially in the Senate. In the House it is, I would say, very commonplace.

But I worry that the Congress itself is very fragmented, that we've had the government oversight committees do most of the work in regards to homeland security. But we have 88 subcommittees and committees. My word, we have to do a better job. So in terms of Senate Resolution 400 I'm concerned about that.

Now that's a laundry list. I'm probably out of time and you've got a yellow light, but if anybody has any comments I would appreciate it.

Mr. HAMILTON. I like the idea of the exercise. I participated in a number of those, Senator Roberts, and you play a role in those exercises, usually a high-ranking Executive branch official. The value of them is it really makes you confront the problem in a very

direct way, and you get opinions coming at you from a lot of your colleagues that give a different perspective of the problem and you find out how tough the decisionmaking process really is.

I like the idea. It's probably the best single educational experience for a Member of Congress to go through, because Members of Congress are not accustomed to thinking like an Executive branch person in making decisions.

Secondly, with regard to the Congress, I agree wholeheartedly. The Congress has to get itself in shape just as much as the Intelligence Community does. You can't possibly conduct oversight of intelligence with 88 committees or subcommittees or whatever it is. That's an unfair burden on the Executive branch to confront that. I think reform of the Intelligence Community, I'm all for that, as I've indicated, but it's not just reform of the Executive branch. The Congress has a lot of reforming to do too.

General ODOM. I like very much the idea of a smaller permanent joint committee. I think that would be a lot more efficient. I think the old Joint Atomic Energy Committee was very effective. I think you inherited this from the mid–1970s, but if you could get back to that I think you would have a much more open relationship with the Intelligence Community.

Mr. HITZ. And remember, Senator, we have a precedent for it. When the oversight of covert action was first passed in the Senate with the Hughes-Ryan bill there were some 12 committees of the Senate or 12 committees of the Congress, rather, that could claim jurisdiction for parts of that information. Eventually, with the creation of the permanent oversight committees it dwindled to two, plus the appropriations committees.

Senator ROBERTS. I thank you. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Senator Roberts.

Senator Feinstein.

Senator FEINSTEIN. Thanks very much, Mr. Chairman. And thank you very much, gentlemen, for your testimony. Mr. Odom, I want you to know I read your op-ed in the Wall Street Journal. We're going to have Director Freeh before us on Tuesday and I look forward to asking him some questions related to it.

Mr. Hamilton, it's great to have you back again. It's wonderful to see you.

Mr. HAMILTON. Thank you.

Senator FEINSTEIN. A very respected member of the House.

When I came to this committee about a year and a half ago and realized the vastness of the intelligence operation of this country and how diffused it is, spread across so many agencies, with nobody really at the helm, it became very apparent to me that a director of national intelligence was really important. So in June I introduced that legislation, which would create a director of national intelligence which would give him program authority and budget authority so that he would have the wherewithal to really oversee this disparate community and to move deck chairs on the Titanic, so to speak.

I sent out a Dear Colleague. I got back virtually no response. It's before this Committee now. One response I did get was from Mr. Tenet, in a letter dated August 27, which, Mr. Chairman, I'd like

to enter into the record, if you would give me permission to do so——

Chairman GRAHAM. Without objection.

[The information referred to follows:]

The Director of Central Intelligence

Washington, D.C. 20505

SSCI # 2002 - 3814

W/02-2732

27 August 2002

The Honorable Dianne Feinstein
United States Senate
Washington, D.C. 20510-0504

Dear Senator Feinstein:

Thank you for your 17 June 2002 letter and for giving me the opportunity to provide views on legislation that you introduced on 19 June 2002 as S. 2645, the "Intelligence Community Leadership Act of 2002". We share the common goal of a robust Intelligence Community (IC). I am concerned, however, that the bill would have the unintended effect of weakening, rather than strengthening, the IC and the Central Intelligence Agency (CIA).

It is my belief that the head of the IC must have a direct relationship with, and more than illusory control over, the CIA. The Director of Central Intelligence's authorities as head of the IC are amplified by the CIA's unique position as the US Government's primary all-source intelligence analytic agency and by its central role in covert actions and liaison with the intelligence and security services of foreign governments. I believe that dissolving these links would weaken the Community. Thus, I cannot support the bill at this time.

After Congress has completed work on the establishment of the Department of Homeland Security, the Administration will be in a position to consider whether changes to the organization of the elements of the IC are needed. I would like to work with you and other interested members in thinking about how the IC can best be structured to meet the national security challenges of the future. This is an important subject, and while I cannot support the legislation you have proposed, it can serve as an important starting point for very thoughtful study, thinking, and debate.

Sincerely,

George J. Tenet

Senator FEINSTEIN. I'd like to read a brief part of that letter and then ask you to comment on it. I think the feeling is genuine and heartfelt. I have a hard time understanding it because the legislation really prevents this from happening.

He says: "We share the common goal of a robust Intelligence Community. I am concerned, however, that the bill would have the unintended effect of weakening rather than strengthening the IC and the CIA. It is my belief that the head of the IC must have a direct relationship with and a more than illusory control over the CIA. The Director of Central Intelligence's authorities as head of the IC are amplified by the CIA's unique position as the United States government's primary all-source intelligence analytic agency and by its central role in covert actions and liaison with the intelligence and security services of foreign governments. I believe that dissolving these links"—which I'm not talking about—"dissolving these links would weaken the community. Thus, I cannot support the bill at this time. After Congress has completed work on the establishment of the Department of Homeland Security the Administration will be in a position to consider whether changes to the organization of the elements of the IC are needed."

Now he offers the rationale. On the other hand, we have this very territorial series of a dozen or so agencies, each of whom relate to various aspects of the State Department, the Defense Department, Central Intelligence Agency, and in this new world we're spending a great deal of money and yet there is no real unity of structure and no ability to tailor the community based on specific needs.

I'd love to have the comments of each of you, if I might.

General ODOM. You see, I think you're overlooking and the committee in general here in this discussion this morning is overlooking the degree of success we have in orchestrating a rather diffuse set of organizations. In the counterintelligence area, where you have the agency in the Attorney General's department and it isn't really an intelligence organization but is a law enforcement organization, and when you combine that with the fragmentation among border control departments, you get a real mess. That's what's caused all the problems.

To conclude from that that you have the same kind of fragmentation problems in the Intelligence Community I think is not valid. I disagree with some parts of this. I don't think that you weaken the community by having the DCI separated from—if you want to call him the director of national intelligence, fine, and I think there's a little misunderstanding here on what we really mean by this. If you mean making the DCI separate from the director of the Central Intelligence Agency——

Senator FEINSTEIN. That's correct. That's essentially it. The DCI could be the DNI, for that matter.

General ODOM. Absolutely. And that I'm very much in favor of doing that, and I think it would be a very—it could be a very effective arrangement. I find technical, legal difficulty and just operational difficulty with giving budget execution authority to this individual inside other departments. Having been under the program management control of a central authority, I find that reasonably effective. I felt very much constrained and kept in line. What I saw

lacking was the inability of the staff under the DCI to structure the input-output relationship so we could get an effective budget together.

And he was the prisoner of the CIA on this, and the NRO and other parochial players, and it's freeing him up to where he will impose a programming, planning, budget structure system that I think will empower him as much as budget execution authority.

Let me say that we draw an analogy between space and intelligence. Everybody thinks that NASA is in charge of space in this country. Space is a place, not a mission. There are many missions in space. The Commerce Department has a mission in space; it's weather. There's a private sector, telecommunications. The universities, science, the Intelligence Community, there are a dozen other missions in space.

Now can you centralize all those under one czar of space in a single department in the U.S. government? No, and it's kind of a mess. If you use the DCI program management model, you'd have a director of space, and he would have to look over every budget where there's space involved and put it together and say am I funding adequately each. Which one should I give a plus-up? And you get an overall comprehensive look, and the Senate then could find out, and the House, what the input-output relations are. He doesn't have to be able to execute those budgets to cause that to happen.

So I think the DCI model, separating the CIA, there is a separation of sorts, even though one person is wearing the hat now, is an accumulation of learning about how to manage this federal system. So I don't think it's in as desperate a shape internally on the foreign intelligence side. I think it is an abject mess on the counterintelligence side.

Senator FEINSTEIN. Just so you know, in my bill there is no inside authority, and I would like to give a copy to each one of you. Perhaps you would take a look at it and make any comments you would care to make.

General ODOM. Be glad to.

Senator FEINSTEIN. Mr. Hamilton.

Mr. HITZ. He's going to kick it to me because he thinks he's been heard on it.

Senator Feinstein, I may be bound a little bit by my long history at CIA and tendency to find some of the arguments in the letter that you read from DCI Tenet to be arguments I've heard and tend to agree with over time. But, as Congressman Roemer has said, and Senator Rockefeller, we have had 9/11. If this isn't a better time to look at this from ground zero, when will there be?

It strikes me, you know, in 1947 you had the creation of the National Security Council, which was intended to do for the President of the United States some of the things that you're talking about putting in the responsibility of a director of national intelligence. It was the National Security Council, on behalf of the Secretaries of State and Defense, the President and Vice President, who were going to tell the DCI how to organize the collection and, more to the point, the analysis and dissemination of intelligence. President Truman was tired of reading 115 million reports.

And it probably isn't possible or desirable to have the national security advisor in effect put in the role of the DNI, but it strikes me that since September 11, with all of the complaints about the inability of the FBI and the CIA to talk to one another, the President of the United States has fashioned a pretty darn good remedy for that. He sits them down in front of him several times a week and says what the heck is going on here and are you guys cooperating.

Now the President can't do that every day. He's got a lot of other things to do. And if your DNI is a person who is going to do that in his behalf, with his authority and with something more than that—and he isn't going to hide behind the White House and fail to come to the Congress to answer your questions on the appropriate occasion, maybe that's something that should be looked at.

But it strikes me that budget authority is one thing, but what General Odom keeps pointing back to, operational, management operational authority, that's the thing that the Secretary of Defense in the current structure is never going to give up when it relates to agencies that are supplying him with information that protects the fighting men. And I can understand his point of view. I just think all of these—the DCI, the SecDef and the Director of the FBI—have got to work together and have got to do a better job and have got to do it in a way that minimizes overlap and confusion, and maybe a DNI can do that on behalf of the President of the United States and still be responsible to Congress in such a fashion that you can get him up here and ask him what he's done.

General ODOM. Can I add one short sentence on that?

Senator FEINSTEIN. It's up to the Chairman.

Chairman GRAHAM. I'm very generous and compassionate, plus I value the information we're getting.

General ODOM. If you had a national counterintelligence service outside of the FBI and the FBI were in law enforcement, what I proposed in my testimony this morning, under the DCI, the DCI would already have these people in the room together. They wouldn't be in another department. And that's how you get the counterintelligence side and the domestic side talking to the foreign intelligence side.

Mr. HAMILTON. Senator Feinstein, I've commented on this quite a bit. I'll just conclude. The thing that puzzles me—I support your idea—the thing that puzzles me here is why we reject for the Intelligence Community the model of organization that we follow in every other enterprise in this country. We have someone at the head who has responsibility and accountability. We accept that. But for some reason we reject it when it comes to the Intelligence Community.

Chairman GRAHAM. Thank you, Senator. It has now rotated back to my time as we finish the first round of questioning. I had asked a question in my first round about ideas to enhance the personnel standards and quality, retention, creativity of the Intelligence Community, and I would be interested in the General and Congressman Hamilton's comments.

Mr. HAMILTON. Senator Graham, we talked a lot in the Hart-Rudman Commission about this problem of personnel. And one of the conclusions we reached was that the personnel or the civil serv-

ice system in the United States has now become a national security issue. We think it is that serious or we thought it was that serious a problem.

I know you are wrestling with this in the Senate right now on the Department of Homeland Security and I don't mean my comments to be directed too much to that. There is too much rigidity in the system. There is not enough allowance for incentive. And it is an exceedingly serious problem in our government. And it has national security consequences. We've got to work through this matter so that managers can manage more effectively.

I've had the experience of running a Congressional office and I've also had the experience, as I am now having at the Wilson Center, of running at least part of my employees there under the federal system. I would absolutely assure you, ladies and gentlemen, that you would not tolerate in your office the kind of management restrictions that operate today in the federal government. You could not run a Senatorial office.

Now I know the importance of this to employees, so it's a tough problem, but the only thing I want to say here, Senator, when you talk about personnel we are now approaching this national security review and we have to look at the civil service system and we have to find ways and means of getting more flexibility into it. If we don't, we're going to choke ourselves to death.

Chairman GRAHAM. Before turning to the General, you mentioned that you became aware of the severity of this problem while serving on the Hart-Rudman Commission. Did that commission make some recommendations?

Mr. HAMILTON. Yes, it did.

Chairman GRAHAM. And did those recommendations basically represent your thoughts as to what should be done?

Mr. HAMILTON. They do. And if you want it in one word, it's more flexibility.

Chairman GRAHAM. General.

General ODOM. I don't have a lot to add. I endorse Mr. Hamilton's points with all the force I can. Dealing with—even with people in the Intelligence Community not necessarily under as free a rein as the rest of the federal service, it's still difficult. I'd much rather have people in uniform. I know how to hire and fire people in uniform. If they're not in uniform, it's hard. You can't hire and fire them. And the intelligence business is warfare. And if you don't look at it that way you're going to be beaten.

I mean, it's not a friendly affair. It's not a negotiating affair. It's you're going to take the other guy or he's going to have you. Would you run the NFL football club that way? Would you choose your quarterbacks on this kind of basis? Well, I don't want to choose my agents, I don't want to choose my analysts on that basis.

Chairman GRAHAM. My time is going to be out soon and I have another major question I'd like to ask which I'm going to hold to the next round. But for this, General, you've talked with wisdom and insight on the specific issue of counterintelligence. Recently there was organized what's called CI–2000, I believe, which is a multi-agency effort at counterintelligence. It is supposed to have a couple of particular qualities—one, to approach counterintelligence in a proactive basis, such as identifying what are the crown jewels

that our adversaries might want to learn and then begin to ask how do we defend those against attack. It also has a heavy emphasis on what I would call benchmarking, trying to ask what are the best practices in the Intelligence Community in things like use of polygraphs to try to enhance our defenses against espionage.

Do you have any comment about that initiative?

General ODOM. I do. The intelligence study that was cited, which you have, that I did in 1997, is being published as a book at Yale Press. It will come out in January. It's been de-acronymized so it's a little more accessible to the public.

I bring up this point and try to clarify what I think is a serious muddle in that kind of proposal. I said earlier counterintelligence is information about the other person's intelligence capabilities and what they are seeing of you. Security is not an intelligence responsibility. Let me put this in a practical case that I lived through.

Most of you remember the Soviet bugging of the Moscow Embassy. My agency had a lot to do with discovering that. I had subordinates who thought they got their instructions from God, protecting the crown jewels, and they were going to go down and make George Shultz shape up, clean up the embassy in Moscow. I had to explain to them that we could make the information available that the KGB was reading his mail. It was his authority to decide whether or not he cared. NSA couldn't do anything about that. But I had really—people were deeply convinced that we needed to do something.

Some were down here lobbying staffs and Members of the Congress on trying to force the Secretary of State to do what he might or might not want to do. My point was, the President hired him and the President's finally responsible for the security. If he wants the Secretary of State to fix the Moscow embassy properly, he should order him to do it. The intelligence people can't do that. A counterintelligence service cannot protect the secrets. Security is a manager's responsibility. He buys the locks and puts them on the doors. He hires the guards.

The intelligence guys, the fellow goes out and finds information. And I've run into these well-meaning people who confuse the security role with the counterintelligence role. And unless you sort that out you will find yourself with organizational muddles you wish you had never gotten in.

Chairman GRAHAM. Thank you, General.

Senator Shelby.

Vice Chairman SHELBY. General, we're not picking on you. We appreciate all three of you and we appreciate Judge Webster too. As a matter of fact, I read again today your article—I had read it back in June—that was published in the Wall Street Journal. I thought it was very interesting and maybe perhaps instructive.

The British have what we call or what they call MI–5, right? How does MI–5 work in the U.K.?

General ODOM. I don't claim to be a great expert on MI–5, but I can tell you what my impressions are. It does counterintelligence, only counterintelligence.

Vice Chairman SHELBY. Nothing else, does it?

General ODOM. Nothing else. It's not a law enforcement agency. It turns to Scotland Yard to arrest people. But it's different from my proposal.

Vice Chairman SHELBY. That's what I wanted you to get into.

General ODOM. It stands out there alone and is a competitor. In my proposal the national counterintelligence service would be under the DCI, just like CIA would be. Number two, MI–5 I do not believe can look into the counterintelligence picture held by MI–6. In other words, MI–6 in its offensive operations will inevitably get into counterintelligence. They'll learn about the other guy's spies. So everybody's going to be doing some counterintelligence.

But this agency which does only counterintelligence needs to look in there so he can see whether there's a gap, whether his agency is being played off against the other one. And I would have—I don't think MI–5 looks into any counterintelligence activities in the Ministry of Defense in Britain. I could be wrong about that.

But what I propose is there would not be counterintelligence operations run in the military services that were not coordinated with the national counterintelligence service. So the national counterintelligence service could look down every one of these closed holes and see what the overall picture looks like. If you can't do that, you're not going to have a comprehensive picture.

It's not to exaggerate. If I were a foreign intelligence service I would love to run against the FBI and the counterintelligence capabilities here. You've just got big gaps welcoming you to come through.

Vice Chairman SHELBY. They've done quite well, haven't they, against the FBI? Why would you want to—and I'm not saying it's good or bad; it's just your proposal—to put this under the DCI or central intelligence as opposed to a freestanding entity?

General ODOM. I want it to be freestanding, away from the CIA. I want it under a Director of Central Intelligence who is not the director of CIA.

Vice Chairman SHELBY. So what we've been talking about is like creating, as Lee Hamilton mentioned, a CEO, a chairman of the board of the Intelligence Community.

General ODOM. It's closer. I think Congressman Hamilton wants more executive budget execution authority than I do. But otherwise I think we overlap enormously. Also, this was my point to Senator Feinstein, that if you're trying to force these people in the room together and you've got the DCI in control of both of them, he can cause them to do that. Counterintelligence is intelligence. They are more closer kin in their skills, their cultures, et cetera to the rest of the Intelligence Community than they are to law enforcement.

Vice Chairman SHELBY. General, how would the other agencies, assuming this counterintelligence agency or entity was created as you would envision, how would the other community, how would they share their information? You know, they would have some information dealing with some counterintelligence, would they not? It's just cross-fertilization.

General ODOM. Absolutely. It's call multidisciplinary as opposed to counterintelligence. They will be a user of the national imagery agency collection. They will be in a position to task the national im-

agery. The FBI, if it wanted to, could do that today under the way the system is organized.

We're talking about a homeland security department. With the present Intelligence Community system, maybe it isn't run very well—I don't know—but when I was there I got a list from all kinds of agencies and I had to put the priorities up there and give those agencies the priority that the DCI put his stamp on. And the homeland security would get it. If FBI—I actually did a lot of support for FBI. That was not the problem.

The problem tends to be where it's a human intelligence kind of activity and CI gets limited entirely, almost entirely, to human intelligence approaches in the FBI. And if it were centralized it would use signals, imagery, the whole thing.

Vice Chairman SHELBY. Mr. Chairman, I know my time is up, but one quick second. You point out, and I think you do it well, General, that there's a heck of a difference between counterintelligence and law enforcement and the methods that you go about it, because you're dealing with a different type of people and you have to have different approaches to it. I commend you for that.

Thank you, Mr. Chairman.

Vice Chairman GRAHAM. Thank you very much, Senator Shelby.

Senator Rockefeller.

Senator ROCKEFELLER. One quick one but important to me. Congressman, you've talked about no corporation would run this way. You've got to have somebody at the top. Mr. Hitz, I'm not quite sure where you stand on that. But I'm just covering the base here with you and I thought I'd find out, and I suspect you lean in that direction, and, General, you too to some degree—accountability.

Throughout a lot of discussions that we've had, both open and closed it has often rattled around the back of my mind that the ultimate consumer on behalf of all of this and the one who has the most to gain and the most to lose if the system isn't operating properly and the one who has the most power, albeit it not legislative but in effect can have an enormous effect on that too, is the President of the United States.

And it mystifies me that when we meet we talk about what kind of legislation can we get passed when all of these commissions that Eleanor Hill talked about this morning put in their two years of work and put out terrific reports and then nothing happens, it's because you're addressing that, in a sense, to the world at large but sort of generally to us and to a fairly elite community that would be interested.

If anybody after 9/11 has to be interested, it's the President of the United States. And if anybody has the power to make certain kinds of changes through executive authority, executive directives, through jawboning, through calling people in and saying I think intelligence, the business of intelligence is one of the three or four most important things that happens in the country today, it is the President. In terms of the survival of the nation along with a good fighting force, intelligence has to be it.

And so therefore what could be more important to him or to her than that? So my question to you is, why is it that the President somehow never comes into our discussions? You know, I gave an interview—it was probably a little bit naughty of me—that, with

all due respect, the President has a lot of authority as to what gets passed and what doesn't get passed in the House of Representatives, on certain subjects. I'm not talking about intelligence but energy and a lot of other things, and taxes and things of that sort. And that defines the power. That's his right.

If he feels strongly about something, that's what he's meant to do. He's the only person elected by everybody and now it's to protect us. So what is it that he could be doing about this?

Mr. HITZ. Senator Rockefeller, that's where I am on the answer to your first question. At the end of the day, the President of the United States has the principal interest, I would say, in getting the intelligence information that he needs to do his job, and on the terrorist side to stay in business. And the difficulty with him being made accountable in the sense that you all are seeking it here is that you don't have the same kind of ability to reach him as you would one of his cabinet officials in terms of calling him up to testify.

But at the end of the day it's the President of the United States who has to make sure that the Director of Central Intelligence, the Director of the FBI, the SecDef, all of them cooperate to do the best job.

Senator ROCKEFELLER. But if there were a conflict that he saw between, as we've talked about today, the 85 percent budget authority for the Defense Department and the 15 percent left over for the Central Intelligence Agency and he found that not helpful to his national security purposes and national intelligence purposes, he would be in a position, I would think, to be able to do something about that. We aren't.

General ODOM. I said earlier to someone's question what do you do, how do you get reform. And I pointed out, I brought the President's name up. The President, the Secretary of State, the Secretary of Defense, if they want to change this, they could change it. They are the users, and for the very reasons you said, they are the source of change if you're going to have it.

But let me point out that intelligence is a support function and it's a specialized kind of activity for an overall operation. When you say there is no corporation in the U.S. that doesn't have a single person in charge, personnel operations are going on everywhere, but we don't have a commander of personnel. And the OPMS runs sort of the federal personnel service but it doesn't hire and fire in all the departments. They do that. So you're dealing with something that is a support function.

And if you begin to differentiate it out too much to where you have budget execution, et cetera, then you really get in trouble with it. But the place where the President can't change this, I think, without your support over here is with the FBI counterintelligence, because that is a statutory agency with certain authorities and I don't think he could write an executive order that takes—maybe he could write an executive order that takes the counterintelligence role away from the FBI.

Senator ROCKEFELLER. But he can encourage us to.

General ODOM. Pardon?

Senator ROCKEFELLER. He could encourage us to do that.

General ODOM. Well, he should do that.

Senator ROCKEFELLER. But he could be helpful in that process. My time is up. I thank you all. I apologize to the Chairman.

Chairman GOSS [presiding]. Thank you, Senator, very much.

I have delayed my questions primarily because I have been summoned in and out a number of times on other matters and I wanted to apologize to you because I think the value added from the contributions are all have made, Judge Webster included, has helped us very much.

We have an extraordinary amount of wisdom in front of us and we have an extraordinary amount of experience, and we take that not lightly. And I'm glad we're able to apply it to the future, the solutions. A lot of good ideas—just the list that Eleanor Hill read of all of the blue ribbon commissions that we've had sort of wrestling with this, using as a benchmark maybe the fall of the Wall—since that time the number of ways we've gone at this question of what is an Intelligence Community and how do we make it work and what's the purpose of it and so forth.

We're in, in my view, a totally expected part of the Washington cycle in this sense, that we've had some extraordinarily good wisdom from some extraordinarily knowledgeable people over the years on what to do about the Intelligence Community, and the threat and the nature of the globe today, and that the sky was going to fall unless. And the record is replete with that. And as we get our very capable staff to go through it we see time and time again, including people in front of me, who have said if you don't get a hold of this one bad things are going to happen. And of course the bad things happened.

So I have two questions. The first question is, how do we get an audience? How do we get an audience? We certainly have the message. We certainly understand the problem and we certainly have some good ideas for fixes. The question is, how do you get that audience. And I don't know and I am just as frustrated as everybody else, because I'm there too thinking I failed, I wasn't able to get that message across either in my time. Even though I saw it, I just couldn't sound the warning. And I feel a lot of us on these oversight committees are feeling that these days and a lot in the Intelligence Community as well, to be sure.

The second question goes to the media question that was brought up—that I think Congressman Hamilton mentioned—of the good old days when there was a very different relationship between the Intelligence Community and the media, and that was basically the twain shall never meet. "No comment" was about as long as a sentence ever got. I remember how far oversight has come since my days in the Agency in the late '50s and '60s, when oversight was a very different thing than the formalized function that it is now.

But the whole problem we have is we're in that Washington cycle where we didn't get our audience so now we've done what we always do; we've gone to the public. And we said intelligence matters, it really does, and we need to have the right kind of capabilities. In order to go to the public, we've had to go to the media, and that of course is dangerous because everybody has a little different slant on it.

So what you see is a phenomenon in front of you that while we understand with some particularity the threat, understand some

very good solutions that might help us, we have got many, many ideas in the minds of our constituency out there about what we should do and how much we should pay for it and where we should go. And it is now a more complicated matter in some ways than it was before, because there are people with agendas to do things differently.

My view has been that it is important to inform the American people because we have got a huge number of debates that certainly Congressman Hamilton will relate to of the frictions that are between us—the question of the intelligence culture of keeping the information flowing versus the law enforcement of prosecutions successfully to put people in jail, the question of need to know and compartmentation versus coordination and cooperation—these are in direct conflict, it seems—of foreign intelligence and no Americans will ever spy on Americans domestically, the question of risk-takers in the field, the friction between the field and headquarters, the don't rock the boat people at headquarters, and the tension of headquarters and field that we always have anyway, the question of Americans have a right to know anything that ought to be guarded. I'm not sure where that's stated exactly, but it's believed that Americans should know everything.

We have the question of the analysts can't do their job unless they have all of the raw data or just some of the raw data that has been by other analysts going on. We have the culture of the users that says the military gets too much of the product. No, the national customer gets too much of the product. We've got to realign the allocations.

There's not a new debate in here that you haven't heard. Nothing I've just said is new. It's just unresolved, and we need to start making some conclusions in some of these things because I think Judge Webster said the main debate we have before us is striking the balance true between being a free society and a protected society.

I don't think we can get there unless we have this debate, and that means we have to enlist the support of the media. So that is the posit I have before you—is how do we have an informed electorate, an informed constituency on this subject, given all those problems, and how do we get that audience that hears us clearly and comes away unconfused and says, of course, go do that? If you can help us with that, I am eternally grateful.

Mr. Hitz.

Mr. HITZ. Chairman Goss, I don't mean to be pulling out an example that is inapposite, but I think you have a model in the deliberations of the Church Committee, much of which are being criticized nowadays, certain aspects. They held long hearings on the matter and began to move a bill in the succeeding Congress. And as they moved the bill they discovered that writing charters for the FBI, CIA, NSA, and elsewhere in the context of the world situation the Congress and the President were facing at the time just didn't make a lot of sense, with thou shalts and thou shalt nots.

And at the end of the day, as you recall, in 1980, a simple two or three-paragraph bit of legislative language was passed causing the Intelligence Community and the Director of Central Intelligence to keep the Congress fully and currently informed about a range of issues. You've taken it from that. And all I'm saying is,

aren't you really saying with the work that you've done you've got some ideas. We've talked about a number of them today—the DNI concept, et cetera. As you move a bill, you're going to find that either support develops for that idea or people come up with some kind of reason why it shouldn't go. It seems to me you are to some degree addressing that audience just by virtue of the legislative undertaking that this is a predicate for.

I mean, I think that's how it's going to come out. And if it doesn't stop with you at the end of this series of hearings and your final report and appears to be going on to a commission which may have a broader ambit, they will, I suppose, have something to say about it too. But you do have, at least where I sit, you do have an audience in the sense of an American public that wants to see what can be done to improve our intelligence and law enforcement performance in this area.

Chairman GOSS. Thank you. Congressman Hamilton.

Mr. HAMILTON. Before I try to respond to the unanswerable question you have raised here, let me say that I think your explanation a few moments ago of the tensions, if you would, between a democratic society on the one hand and intelligence on the other was a very, very good statement.

Chairman GOSS. Thank you.

Mr. HAMILTON. And it reflects how, as I said in my statement, how awkward it is for the intelligence function to fit in a democratic society. Two or three comments.

You asked how do you reach an audience. The answer to that in part is that the audience you want to reach is a very elite audience. Most people aren't interested in intelligence. I think they are more interested in it after September 11 than they were before, and they are beginning to see the importance of it. But what we've been talking about today is an insider's game and so the audience is not vast out there, I believe, and therefore should be somewhat easier to reach.

Having said that, I hope I don't contradict myself by saying that I do think it's very important to reach out to the public. You're doing that in these hearings, which are public, but I must say, Mr. Goss, I'm not sure but if you look over the last decade or so and saw the number, the percentage of open hearings the Intelligence Committees had in the House and the Senate, it would be fairly small.

Chairman GOSS. Very small.

Mr. HAMILTON. Because most of your business has to be done in secret. I'm not critical of that; it's just a fact. We've had CIA directors in the past who were really interested in the problem you raise. Bob Gates comes to mind. And Bob, Mr. Gates, made an extended effort. I went with him, as a matter of fact, around the country giving speeches together—one legislative viewpoint, his the Executive branch—on the Intelligence Community. And we went to a number of college campuses and there was enormous interest in that.

In other words, here was a CIA director who was concerned about the kind of things you're talking about who really made it a point, with all of the CIA director has to do, to reach out to the American people. In this case he went to a lot of campuses to tell

people about the intelligence function. Well, I think that's a very important part of it.

The third point I'd make is that there is value in the debate itself even if you don't reach a conclusion. I really think that's the case. We've all seen that in the democratic process. The mere fact that General Odom and I may have a difference of opinion about what you do with the DCI, we're not probably going to resolve that to either one of us's satisfaction. But the fact that you discuss it is important and makes each one of us more sensitive to the other's point of view, which I think has been terribly important here.

The final word would be George Shultz's statement, who said nothing is ever finally decided in this town. And there's a lot of truth in that.

Chairman GOSS. Thank you. General.

General ODOM. I would just make two points. I think Senator Rockefeller has already preemptively answered a lot of your questions. You don't need a big public audience to get these things done. You need the people in charge who use the intelligence to do it. So I even have wonderment about this endeavor in this way.

Second, that takes me to my second point. May be we didn't have the information because the trend over the past ten or twelve years and even more recently has been to make our intelligence activities a lot more transparent. I could tell you as an intelligence operator if I were running al-Qa'ida, with what I could read in the American press, I could see how to evade you. So I think the publicity approach to intelligence ought to be seriously scrutinized in light of the intelligence failure vice 11 September.

Chairman GOSS. My time has long expired. That's a subject of great debate. Can a democratic, free, open society that plays by the Marquis of Queensberry rules exist in a globe where not everybody else is playing by the Marquis of Queensberry rules. But my time has expired and I'd love to take that up in chapter two.

Chairman GRAHAM [presiding]. We have now completed round two and we're now at round three, which I think will be the conclusion of our imposition on your time.

The question I wanted to ask, which has haunted me from September 11 and before September 11 but particularly since then, it seems as if the Intelligence Community had a difficult time recognizing that the cold war had ended and that some of its practices which were the product of the cold war were not relevant or not the most relevant to the new world in which the Intelligence Community would be called upon to provide information to decision-makers.

I would put just as a few characteristics of that failure to evolve the fact that we had big struggles over whether to use a satellite architecture that seemed to be more aligned to continuing to look at the Soviet Union rather than the flexibility to look at multiple issues, the continued decline in human intelligence which had started at the end of the cold war and continued after the cold war, when it would appear that the nature of our adversary would be such that we need more emphasis on human intelligence, some of the problems that NSA had in the 1990s, including one period where it went black for a while, with it said that our technology was falling behind the technologies with which we had to compete.

A—do you believe that in fact we have what I call the Darwinian problem of failure to recognize that the environment in which we're living is changing and by that failure almost consign ourselves to a death spiral and, B—if that is an accurate, maybe a little overdramatized, statement, what can we inject into these big intelligence agencies to give them a great capacity to recognize changes and to respond to them? Because it's my thesis that if there's been significant change in the world in which the Intelligence Community operates since the end of the cold war, if you project an equivalent period of time into the future there will be even more change during the next eleven or twelve years.

So what can we do to try to not require a 9/11 incident to shake us that the world is changing and we need to change and adapt to it or we will die of irrelevance?

Mr. HITZ. Well, if I may be so bold as to start, I lived through part of it, Mr. Chairman, as did all of you on the dais. And the shift over after '91 I think you are accurate in saying took a long time.

Part of it—and there's no blame to be levied here—part of it was the notion that the Intelligence Community thought it, like the military services, was going to pay a peace dividend. We cut back substantially on the recruitment of new personnel. We wanted to get smaller. When we did that, with the whole changeover in targets that Presidential Decision Directive 35 led us to, a good many seasoned operatives decided they had won the cold war, they had enjoyed working against the Soviet target, and they didn't necessarily want to shift over to the next sets of targets.

At the same time, we were going through—again it just happened that way—a revolving door at the top of CIA. I served, in the period of eight years, under five different Directors of Central Intelligence. That's an awful lot of change at the top of a major corporation. And each Director, in good faith, had his own ideas of how he wanted to do the job and sent out a lot of directives and stirred up a lot of commotion, as happens in a bureaucracy. So we were slow on that, but 9/11 was the wakeup call and, as I'm sure it's been chronicled before this Committee to an extraordinary degree the response has been heartening in the sense that new people have applied. The new targets have been measured.

But there was a lot of time lost.

Mr. HAMILTON. I would agree that the community, Intelligence Community, has had a lot of rigidity in it and has been slow to change. It focused early on, for example, a few years back principally on an attack by ballistic missile and there were a lot of other things out there other than ballistic missiles and we learned about them, to our regret. It focused very heavily on military threats and overlooked the terrorist threat for a long time.

It was focused on advanced technologies and overlooked the importance of the human spy. It focused on collection and not enough on analysis. It had a lot of bureaucratic rigidities.

Now all of that is in the past, all of that I think is conventional wisdom that we need corrections there. How do you bring about those corrections? Well, you bring them about exactly the way you've been doing. You've been calling people in here from the Intelligence Community and pointing out a lot of these things to

them and changes are beginning to occur. When a Director of the FBI comes in and says we're going to start emphasizing prevention instead of law enforcement, that's a revolution. Now it's going to take a while to carry it out, but it's quite a change.

So things are happening and I think they're happening positively. The process works too slowly, I am sure, for all of us, but your job, which I think you are fulfilling is to call these people up here and put them on the spot and let them know what you think the changes are that are occurring in the world and in the country, put a little sunlight on it, make them respond. And the system will move, maybe a little too gradually, a little too slowly, but it will move.

General ODOM. The comment I would add to this is to make a distinction between policy issues and structural issues. The hearing started out focusing on structural issues, and most of Mr. Goss's comments, those were policy issues more than structural issues.

We're going to make mistakes, and that's corrective feedback. Sometimes you pay a higher price, sometimes you pay a smaller price. In the military we have a tradition. When you screw things up, we relieve the commander, which leaves me puzzled about the behavior of the Administration in the intelligence area. I consider intelligence, as I said earlier, a military engagement, and I would hold the commanders as responsible as I would ship commanders who run their ships aground. They don't stay around after they've run them aground, even if they are not very guilty.

And I've seen people relieved in Vietnam who you wouldn't believe how little they were relieved for. But the example turned out to quicken the responsiveness of people below. So I think that's the policy issue you're facing on the redress here.

The business of shifting adequately, I didn't live through it, but let me explain some of the things I know about it just from old friends and hearsay. You had these big organizations. They had to make programmatic decisions to downsize. They didn't do that very well, in part because of internal management incompetence and also because the community at large does not have a PPBS system. It has a kind of everybody's playing, pulling his chips in and trying to beggar the other fellow.

And the DCI, unless he builds some kind of system to do that, you're not going to improve that very much. This is a structural issue, and it was the second point of my comments in my statement this morning, how you relate input dollars to intelligence output. And the absence of that system I think explains some of the slowness and viscous reactions within my old Agency, NSA, and other parts of the community in the 1990s.

Chairman GRAHAM. Congressman Goss.

Chairman GOSS. No.

Chairman GRAHAM. Senator Rockefeller. Mr. Condit.

Mr. CONDIT. Mr. Chairman, I can't resist this. I know it will get a rise out of the panel, but I want to go back to the comment the General made about transparency. I don't have the benefit of serving in the Intelligence Community like some of you have and Chairman Goss has, but it just seems to me what's the problem with opening this up? I mean, everybody knows that everybody's watching everybody and that we're going to monitor people, we're

going to monitor weapon systems, we're going to monitor actions and so on and so forth.

If there was more transparency it just seems to me it would be more openness, more sunshine on the issue, everybody would be aware of what's going on. And the fact is, as we're doing the terrorist thing right now there's not much that is not in the newspaper already about what goes on with that. So why wouldn't we just 'fess up and just say this is what we're doing, this is what we're going to do, and if we catch you doing this we're going to do this? Why wouldn't we do that? It seems to me it's an honest approach to protecting ourselves but doing it in a transparent way so that people know we are.

General ODOM. Let me answer that very briefly. If we did that, we don't need the Intelligence Community. That's called a news service. We have a lot now. I'd say 90 percent of the intelligence that affects policymaking in the government comes out of the media. The media is our best new collection agency. Even some military collection comes out of it.

General Vessey, when he was Chairman of the Joint Chiefs, would look over at the television and see CNN on someplace and say, Bill, why can't you do that for me. Well, I said, I don't need to because CNN is doing it free. And the Intelligence Community really needs to take advantage of that. We should.

The second point is, people have short memories and even though something's published and made information today, they don't keep it in mind. And what they are exposing, what they close up from having been alerted, sometime later they may open up again. And if you go around reemphasizing openness you keep educating them how to defeat your intelligence collection.

Mr. HAMILTON. Mr. Condit, I think there has been over a period of years a kind of set of mind in the Intelligence Community to keep more secret than is necessary, feeling that we know best how to handle this and it's not a matter that really should be discussed in public.

I think the Congress and the oversight committees have done a lot to try to change that perception on their part, and my view would be you want to maximize openness and transparency to the extent that you can. But you do have to recognize you are dealing with a very special business and you do have to be careful about methods and sources and all of the rest of it.

So it's not an easy kind of a balance to strike. In general, I think the Intelligence Community has erred on the side of too much secrecy and not enough openness. I do think that's changing now, in part because of the Congress and the oversight. There needs to be a greater appreciation by the national security community that the more information that is out there about their job and how tough it is to do, the obstacles they confront, I think the American public understands that pretty well, especially in light of September 11.

But I agree with your premise that more transparency is needed, with a very major caveat that you are dealing with a special business here.

Mr. HITZ. I tend to echo that. For the one or two percent of information that is acquired from a source or by a technique that we would not want to have revealed in order to be able to use it again,

I'm sure that we go to a great extreme to protect things that don't need to be protected. But you do have to protect that essential core.

Mr. CONDIT. I agree with that point. I just also would underscore that it seems to me all the work that the three of you and Judge Webster have done on making suggestions, that transparency may be the thing that forces us to make the necessary changes to reform the Intelligence Community, and it's the very thing that we seem to frightened of. I just think we maybe should take a look at embracing it a little more than we have in the past.

I thank you.

Chairman GRAHAM. Thank you, Mr. Congressman.

Again, thank you to each for your very significant contribution today. We have learned a lot from the wise men, and I anticipate that you will represent a well of wisdom and insight that we will want to come back to again. Thank you very much.

[Whereupon, at 4:05 p.m., the hearing was adjourned.]

HUDSON INSTITUTE

October 11, 2002

MEMORANDUM FOR SENATOR FEINSTEIN

FROM WILLIAM E. ODOM

SUBJECT: "The Intelligence Enhancement Act of 2002"

I fully support the concept of separating the position of the Director of Central Intelligence from the Director of the CIA. I have elaborated my reasons in detail in the reform study, "Modernizing Intelligence: Structure and Change for the 21st Century." This can be done with or without legislation, but it makes no sense unless several other things are done at the same time, things your legislation does not include.

Most important for making the separation work is the creation of three "national program managers" for the three collection disciplines, SIGINT, IMINT, and HUMINT. If it is not, then the CIA remains a mixed and confused organization, and its behavior will not improve.

The National Reconnaissance Office must also be reformed, taking away its independent budget and placing its funding in the hands of the three national managers for SIGINT, IMINT, and HUMINT. The NRO should not be allowed to come to Congress for a budget, but rather depend upon NSA, NIMA, and the CIA requesting and justifying in a "planning, program, budgeting system" monies which the NRO spends to acquire technical collection systems.

No less important is that the DIC – or DNI – has an organization directly under him consisting of 1) a management staff, and 2) a collection, analysis, and production staff. The National Intelligence Council and the DI of the CIA should become the second of these.

Finally, a new National Counterintelligence Service (NCIS) needs to be created with overall responsibility for counterintelligence. The FBI should be taken out of counterintelligence work entirely and left to law enforcement and criminal investigation. The NCIS should be under the new DNI or DCI and authorized to review and coordinate the CI operations of the CIA and the three military departments in the Department of Defense.

Washington DC Office
1015 18th Street, N.W.
Suite 300
Washington, DC 20036

202.223.7770
202.223.8537 Fax
www.hudson.org

Senate Feinstein
October 11, 2002
Page 2

Your legislation, if it does not include these additional structural changes, could produce more problems than it solves. If it goes ahead to include them, it would be a major achievement, on the level of the National Security Act of 1947.

Two other lesser points are worth making.

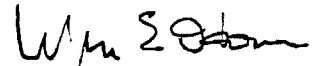
First, on a ten-year term for the DNI (or DCI). I have a mixed reaction to this aspect of your legislation. If an effective choice of a DNI is made, it would be good, but if a weak or incompetent choice is made – more likely – then the country would be stuck with a mess for a long time. Also, the record of the FBI with its autonomous director does not encourage me to have confidence in such a solution. Political accountability for the chief of the US Intelligence Community is important. It already has a large corps of professionals who give considerable independence of mind. The largest part of it is in uniform. And several flag officers serve in its top ranks. Finally, the Chairman of the Joint Chiefs of Staff does not have a ten-year term, and that seems to work well. I could support a similar solution for the DNI/DCI. It might even make sense to require that a military officer hold this post if one wants to depoliticize it, but a very long term could lead to great politicization, as we saw with J. Edgar Hoover.

Second, on budget authority, your bill needs to consider the deeper implications of DNI budget controls. This is a complex issue which I spell out in my reform study. As your bill now reads, I do not believe it would make the DNI follow a "planning, program, budgeting system" (PPBS), but would rather discourage that outcome. I say this because I know you strongly support PPBS being applied to the National Foreign Intelligence Budget. It can be only if structural changes of the kind I outlined above for "national managers" and effective staffs under the DNI/DCI are made.

The budgeting area is a labyrinth of problems. I will be glad to discuss them with you, but they cannot be dealt with briefly in a letter.

Overall, I congratulate you on the main thrust of your bill because it certainly addresses the most visible structural issue: the double-hatting of the DCI and the Director of the CIA. Fixing the problem, however, requires deeper changes than merely separating the two.

Sincerely,



William E. Odom
LT GEN, USA, Ret

T2U2081400I 1-114 P.002/002 F-822

Woodrow Wilson
International
Center
for Scholars

LEE H. HAMILTON
Director

October 11, 2002

Alonzo M. Robertson
Joint Inquiry Staff

BY TELEFACSIMILE

Dear Mr. Robertson

Thank you for your letter of October 7 regarding Senator Feinstein's introduced legislation. I concur with the legislation, and believe that the "Intelligence Enhancement Act of 2002" would address key organizational problems within the intelligence community, particularly with regard to the creation of a Director of National Intelligence. Please convey to Senator Feinstein my support and admiration for her efforts – I know what a tough road this can be.

I commend the work that the Joint Committee has done in conducting this inquiry, and thank you again for the opportunity to testify.

With best wishes, I am

Sincerely,

Lee H. Hamilton

ONE WOODROW WILSON PLAZA, 1300 PENNSYLVANIA AVENUE, NW, WASHINGTON, DC 20004-3027 T 202 691 4000 F 202 691 4001 WWW.WILSONCENTER.ORG

JOINT COMMITTEE HEARING ON THE INTELLIGENCE COMMUNITY'S RESPONSE TO PAST TERRORIST ATTACKS AGAINST THE UNITED STATES FROM FEBRUARY 1993 TO SEPTEMBER 2001 IN REVIEW OF THE EVENTS OF SEPTEMBER 11, 2001

TUESDAY, OCTOBER 8, 2002

U.S. SENATE, SELECT COMMITTEE ON INTELLIGENCE, AND U.S. HOUSE OF REPRESENTATIVES, PERMANENT SELECT COMMITTEE ON INTELLIGENCE,

Washington, DC.

The Committees met, pursuant to notice, at 10:10 a.m., in Room 216, Hart Senate Office Building, the Honorable Porter Goss, Chairman of the House Permanent Select Committee on Intelligence, presiding.

Senate Select Committee on Intelligence Members Present: Senators Graham, Shelby, Feinstein, Roberts, Rockefeller, DeWine and Thompson.

House Permanent Select Committee on Intelligence Members Present: Representatives Goss, Pelosi, LaHood, Roemer, Bereuter, Castle, Boehlert, Burr, Chambliss, Harman, Condit, Reyes, Boswell, Peterson and Cramer.

Chairman GOSS. I call to order the Joint Inquiry of the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.

Welcome to this hearing of the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. This is the eighth public hearing by our committees as they conduct their joint inquiry into the Intelligence Community's performance regarding the September 11, 2001, attacks. The committee has held 11 closed hearings.

Our objective today is to provide a broader context for understanding the events of September 11 and, to that end, today's hearing will focus on lessons that the Intelligence Community learned or should have learned from the terrorist attacks against the United States that preceded September 11, 2001.

Although the September 11 attacks were unprecedented in magnitude and devastation, terrorism is not a new problem for the United States. We are seeking to learn what steps were taken in response to past attacks and what problems hindered a more effective response to terrorism.

Today's hearing will be in two parts. First, we will hear from Eleanor Hill, the Staff Director, who will present a staff statement that reviews the Intelligence Community's response to past attacks. We will then hear from a panel of distinguished witnesses, our former Senate colleague, Warren Rudman, Judge Louis Freeh, Mary Jo White and Dr. Paul Pillar, whom I will introduce more fully after Ms. Hill's presentation.

I will now ask my colleagues—Chairman Graham, Ranking Member Pelosi and Vice Chairman Shelby—should they have any introductory remarks today.

Chairman Graham.

Chairman GRAHAM. Thank you, Mr. Chairman. I do have an opening statement.

I would like to take a moment to discuss what I hope will be a primary focus of today's discussion, what I believe to be one of the major challenges facing our national security infrastructure, including the Intelligence Community. That is, what steps should be taken to increase domestic security against terrorist operatives who are inside our country, having been recruited, trained and placed to await instructions to strike.

I, for one, am deeply concerned that at a recent hearing of the Senate Select Committee on Intelligence, at which we had representatives from the FBI, the CIA and other agencies, there was an alarming lack of information on this subject. The committee was unable to secure satisfactory answers to questions such as the number of foreign terrorists who are in our homeland, their training and capabilities, their support systems, both financial and strategic, including possible support from foreign governments and the command and control systems that might be in place behind them. By that I mean their linkages to their organization's headquarters, generally in the Middle East or Central Asia.

All of those questions are central to our government's ability to disrupt and deter terrorist plots, yet the Intelligence Community seems to be unable to give satisfactory answers. For example, when asked how many so-called "sleepers" of one prominent terrorist organization are operating within the United States, we were given two widely different estimates. One number, from the CIA, was described as an "intelligence estimate"; the other, from the FBI, was said to be "based on active law enforcement cases." There was a chasm between them, an unacceptable chasm in my opinion.

I am especially concerned because we are entering a period during which our President's policies in the Middle East are creating heightened tensions and heightened anti-American sentiment. At last Thursday's hearing of the Joint Inquiry Committee there were various suggestions for the creation of a separate agency within the Intelligence Community to conduct domestic surveillance. There were parallels drawn to the domestic intelligence structure in Great Britain and other foreign countries.

I would like to hear from today's witnesses what approach they would recommend in this critical period, both near-term and long-term solutions. Should we look towards devoting additional attention and resources to this problem within our existing intelligence infrastructure, or should we be creating a new entity for this purpose?

Our ultimate concern and our ultimate goal is to assure the greatest possible security for the American people.

Thank you, Mr. Chairman.

Chairman GOSS. Thank you, Mr. Chairman.

Ranking Member Pelosi, welcome.

Ms. PELOSI. Thank you, Mr. Chairman. I will not have an opening statement except to associate myself with the welcome that you and our distinguished Chairman Graham presented to the witnesses. We look forward to their testimony today.

I wish to associate myself with your and Mr. Graham's opening remarks, especially the list of concerns put forth by Senator Graham. I have concerns about us—except to the point of the separate entity; I have serious concerns about that. While it is true that our ultimate goal is to provide maximum security for the American people, I know our Chairs and ranking members share the view that we must do so while protecting our civil liberties.

With that, I welcome our distinguished witnesses and look forward to their comments.

Thank you, Mr. Chairman.

Chairman GOSS. Thank you, Ms. Pelosi.

Vice Chairman Shelby.

Vice Chairman SHELBY. Mr. Chairman, I do not have an opening statement. I will be brief.

I do want to commend you and Senator Graham for having these open hearings. I believe, although we cannot talk about everything in open hearing—there are a lot of things we shouldn't talk about and will never discuss—there is a lot of information that will be brought out that the American people need to know about.

I want to commend our Staff Director, Ms. Hill, for bringing a story together, and this is a story that is a big challenge to our Intelligence Community and to us as Americans as far as security is concerned. Without these open hearings, I think a lot of Americans would not have any idea what was going on or what we were trying to do to make our Intelligence Community work together better, to make them stronger for the security of our Nation.

Thank you, Mr. Chairman.

Chairman GOSS. Thank you, Senator Shelby.

At this time I ask Ms. Hill to proceed with her prepared statement. The floor is yours, Ms. Hill.

Ms. HILL. Thank you, Mr. Chairman. I have a longer—actually I have two longer versions of this statement for the record. One is a classified version, which I would ask be made part of the sealed record.

Chairman GOSS. Without objection.

[The classified statement of Ms. Hill was made a part of the classified record.]

Ms. HILL. The other is an unclassified version, but longer than the summary I will read here this morning.

Chairman GOSS. Without objection in both cases.

[The prepared statement of Ms. Hill follows:]

Joint Inquiry Staff Statement

Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993 to September 2001

Eleanor Hill, Staff Director, Joint Inquiry Staff

October 8, 2002

Introduction

Mr. Chairman, members of the two Committees, good morning. The purpose of today's hearing is to review past terrorist attacks – both successful and unsuccessful -- by al-Qa'ida and other groups against the United States. This review focuses not only on the attacks themselves, but also on how the Intelligence Community changed its posture in response and on broader themes that demand close scrutiny by the Committees. This review of past attacks and issues is not as deep or as thorough as our inquiry into the events of September 11. Instead, it represents a more general assessment of how well the Intelligence Community has adapted to the post-Cold War world, using counterterrorism as a vehicle.

In conjunction with the Joint Inquiry Staff's (JIS's) review of the September 11 attacks, we have reviewed documents related to past attacks and interviewed a range of individuals involved in counter-terrorism in the last decade. The documents include formal and informal "lessons learned" studies undertaken by different components of the Intelligence Community and the U.S. military, briefings and reports prepared by individuals working the threat at the time, and journalistic and scholarly accounts of the attacks. Interviews included officials at the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Department of Defense (DoD), National Security Council (NSC), Department of State, outside experts, and other individuals who possess first-hand knowledge of the Intelligence Community's performance or who can offer broader insights into the challenge of counterterrorism.

This Staff Statement is intended to provide the two Committees with lines of inquiry that we believe are worth pursuing with the panelists who will appear before you today. It has four elements. First, we review briefly several major terrorist attacks or plots against the United States at home and abroad. Second, we note several characteristics of the terrorism challenge that became increasingly apparent in the 1990s. Third, we identify a number of important steps taken by U.S. intelligence and other agencies to combat terrorism more effectively – steps that almost certainly saved many lives. Fourth and finally, we describe in detail several problems or issues apparent from past attacks, noting how these hindered the overall U.S. response to terrorism. Several of these issues transcend the Intelligence Community and involve policy issues; others were recognized early on by the Intelligence Community but were not fully resolved.[1]

A Review of Past Attacks

The Joint Inquiry Staff has reviewed five past terrorist attacks or attempts against the United States as part of its inquiry into September 11: the 1993 bombing of the

[1] This review is focused on issues that are not addressed fully in other open or closed joint Committee hearings. Thus, for example, important concerns such as information sharing and covert action are not addressed, even though they were important issues in how the Intelligence Community responded to past attacks. This Joint Inquiry Staff has prepared or will prepare assessments of these issues as separate documents.

World Trade Center (WTC I); the 1996 attack on the U.S. military barracks Khobar Towers, in Saudi Arabia; the 1998 attacks on U.S. Embassies in Africa; the 1999 "Millennium" plot; and the 2000 attack on U.S.S. Cole.

The Joint Inquiry Staff chose to review these five attacks for several reasons. First, they suggest how the radical Islamist cause grew from a disparate band of relatively unskilled amateurs to a seasoned group of skilled operators. This span of time allows the Joint Inquiry Staff to determine how the Intelligence Community adapted to meet this danger. Second, the attacks represent the major instances of international terrorism against the United States in the decade preceding September 11, 2001. Third, they represent a mix of attacks on U.S. interests at home and abroad. Finally, we included the attack on Khobar Towers to avoid drawing too many lessons from Sunni Islamic extremists linked to al-Qa'ida: as the 19 American dead at Khobar demonstrates, the Lebanese Hezbollah and other groups also threaten American interests today.

A brief review of each incident is provided below.

1993 Attack on the World Trade Center

On February 26, 1993, a truck bomb exploded in the B-2 level garage of the World Trade Center in New York City, killing six people and wounding another 1,000. The vehicle was traced to Mohammed Salameh, a Palestinian with Jordanian citizenship. Salameh's arrest led investigators to his accomplices – Arabs of different nationalities who were followers of blind radical Egyptian cleric Omar Abd al-Rahman. Ramzi Yousef, the mastermind of the attack, had already fled the United States and was not apprehended until 1995. Yousef's collaborators, who were far less skilled and professional, were arrested shortly after the bombing.

Several of the radical Islamists responsible for the bombing had conducted terrorist attacks before. Members of New York's Joint Terrorism Task Force (JTTF) traced Salemeh to the home of Ibrahim el-Gabrowny, a cousin of El Sayyid Nosair. Nosair was the shooter in the 1990 assassination in New York City of Rabbi Meir Kahane, the controversial founder of the Jewish Defense League. Nosair also had assistance from Mahmud Abouhamila, who was arrested in connection with the first World Trade Center bombing.

According to FBI officials who were interviewed, the NYPD and the District Attorney's office resisted attempts to label the Kahane assassination a "conspiracy" despite the apparent links to a broader network of radicals. Instead, these organizations reportedly wanted the appearance of speedy justice and a quick resolution to a volatile situation. By arresting Nosair, they felt they had accomplished both.

Nosair was shot and then arrested after the Kahane shooting, and a search of his residence uncovered a trove of information regarding his cell's members and activities. Forty-seven boxes of notes and paramilitary manuals were carted away. It would be at least two years before much of the information was actually translated. The FBI case agent says that a relative of Nosair's traveled to Saudi Arabia to obtain money to pay for

Nosair's defense. He received funds from a wealthy Saudi, Usama bin Ladin. The agent told the Joint Inquiry Staff that this was the first time the FBI's New York office heard bin Ladin's name.

According to FBI agents interviewed by the Joint Inquiry Staff, intelligence on individual members of the cell who committed the attack was considerable before the World Trade Center attack. In 1989, the FBI had become aware that a number of Americans were being recruited to fight in Afghanistan in the war against the Soviets, a possible violation of the U.S. Neutrality Act. The FBI also learned that these individuals were receiving firearms and martial arts training in the New York area, and the FBI began to surveil these firearms training sessions. The FBI had an informant with access to the cell but, in essence, deactivated him shortly before the bombing. However, there was no indication of the magnitude of the attack they were planning or that they intended to kill thousands of Americans.

After the World Trade Center attack, the FBI reactivated the source who reported on the cell's plans. Drawing on this source, several weeks after the World Trade Center attack, the FBI arrested additional Islamist radicals planning a "day of terror" against several U.S. landmarks. The source enabled the eventual arrest and conviction of Shaykh Abd al-Rahman and his associates for planning the "day of terror."

A senior FBI terrorism analyst told the Joint Inquiry Staff that the lack of a state sponsor of these terrorist activities and the mixture of nationalities involved in the various plots initially confused U.S. investigators. One FBI investigator recalls that he initially suspected Serbian involvement, and later the prevailing opinion was that Libyans were behind the activity. Others thought that perhaps the Iraqis were seeking revenge for Operation Desert Storm. This theory gained support when it was discovered that Ramzi Yousef traveled with a valid Iraqi passport. Over time, however, the Intelligence Community realized that a new phenomenon was emerging: radical Islamic cells, not linked to any country, but united in anti-American zeal.

1996 Attack on Khobar Towers

On June 26, 1996, Saudi Shi'a Muslim terrorists detonated a truck bomb containing 3,000 to 5,000 pounds of explosives on the perimeter of the U.S. apartment complex called Khobar Towers at a military facility in Dhahran, Saudi Arabia. Although the truck did not pass through the base's perimeter security, the bomb's large size, which surprised U.S. officials, led to a massive explosion that destroyed much of the complex. Nineteen Americans died and 500 others were wounded. Following the attack, the United States redeployed its forces to more remote parts of the Kingdom.

A U.S. indictment brought in June 2001 charged that the Saudi Hezbollah, with support from Iran, carried out the attack. According to the indictment, Iran and its surrogate, the Lebanese Hezbollah, recruited and trained the bombers, helped direct their surveillance, and assisted in planning the attack.

Warning that U.S. forces were at risk of a terrorist attack was considerable, though detailed information on exactly where or when the attack would occur was lacking. The Intelligence Community warned in a series of briefings and written products that terrorists would seek to strike U.S. forces in Saudi Arabia and that the Khobar Towers complex had been surveilled. As the Task Force led by General Downing that reviewed the attack after the fact noted:

> Overall, the intelligence provided commanders warning that the terrorist threat to U.S. service members and facilities was increasing. As a result, those responsible for force protection at Khobar Towers and other U.S. government facilities in Saudi Arabia had time and motivation to reduce vulnerabilities.

A review of the classified version of the Downing report, CIA documents, and interviews with U.S. officials supports this assessment.

1998 Embassy Attacks

On August 7, 1998, al-Qa'ida terrorists bombed the U.S. Embassies in Nairobi, Kenya, and Dar Es Salaam, Tanzania. The attacks, which occurred less than ten minutes apart, destroyed the facilities and killed 12 Americans and over 200 Kenyans and Tanzanians. More than 4,000 were injured, many permanently blinded. Local security forces detained several lower-level perpetrators, and others were caught as they fled, leading to important confessions. Four perpetrators were prosecuted in the United States for their role in the bombings. However, several of those who authorized and helped orchestrate the bombings went to Afghanistan or otherwise did not face justice.

Intelligence warning of the attack was limited. The *Report of the Accountability Review Boards on the Embassy Bombings in Nairobi and Dar Es Salaam* (known as the "Crowe Commission") found that: "[t]here was no credible intelligence that provided immediate or tactical warning of the August 7 bombings." Reporting was imprecise as to location and date, and – in contrast to the steady stream of warnings before the Khobar Towers attack – the Crowe Commission noted that: "[i]indeed, for eight months prior to the August 7 bombings, no further intelligence was produced to warn the embassies in Nairobi and Dar Es Salaam." The Intelligence Community quickly determined that al-Qa'ida was responsible for the attacks after they occurred.

Interviews of Intelligence Community personnel suggest that more than any other al-Qa'ida attack before September 11, the near-simultaneous bombing of the Embassies changed how the Intelligence Community perceived the threat of terrorism from that group. Almost all terrorism analysts at all agencies the Joint Inquiry Staff interviewed appear to have recognized that the attacks clearly demonstrated al-Qa'ida's reach, ability to conduct simultaneous attacks, and determination to kill many Americans. Moreover, the attacks indicated al-Qa'ida's patience: planning for the Kenya operation began in 1993. Before these attacks, only small pockets of the U.S. Government recognized the danger al-Qa'ida posed. After the attacks, the danger was far more clearly understood. On August 20, 1998, President Clinton authorized cruise missile strikes on the al-Shifa

plant in Sudan and on a terrorist training camp in Afghanistan to retaliate for the bombings. Mr. Berger also testified that the President sought to kill Bin Ladin with the missile strikes, indicating the White House's understanding that Bin Ladin was an adversary who must be eliminated.

Planned Attacks Around the Millennium Celebrations

U.S. customs, law enforcement, and intelligence officers successfully disrupted a series of attacks planned around the Millennium celebrations. On December 13, 1999, an alert U.S. Customs Inspector, pulled over an automobile driven by a 33 year-old Algerian, Ahmed Ressam. Ressam panicked and attempted to flee; he was caught, and inspectors discovered explosives in his car along with a map on which two airports in California and one in Ontario were circled, according to *Through Our Enemies' Eyes* (Brasseys, 2002), a book by an anonymous senior intelligence official. As Ressam was being arrested and questioned, planned attacks on tourist sites in Jordan were disrupted, and 22 Islamists were eventually convicted on terrorism charges. Ressam was convicted in the United States on terrorism charges in April 2001.

Following these discoveries, the Intelligence Community and the FBI coordinated a worldwide disruption effort to disrupt other possible attacks. The effort involved dozens of foreign intelligence services that detained suspected radicals in the hopes of gaining confessions or at least keeping them off the streets or intimidating them into aborting any planned attacks. Louis Freeh, the former FBI Director, also related that FBI agents also arrested suspected radicals in the United States for minor violations (often linked to visa problems) and tried to disrupt any planned attacks in the United States.

Following the disruption, the Intelligence Community clearly warned senior policy makers that the disruptions only bought time: they did not end the threat of future attacks. Of interest is another attack planned for around the Millennium that went undiscovered – the planned January attack on another Navy warship. The plot failed because the terrorists' boat sank, not because the Intelligence Community disrupted it, and a similar attack was carried out on *U.S.S. Cole* in October of 2000.

2000 Attack on *U.S.S. Cole*

On October 12, 2000 al-Qa'ida terrorists piloted a small boat filled with explosives next to the destroyer *U.S.S. Cole* in the harbor in Aden, Yemen, and detonated it, killing 17 sailors and wounding 39 more. The bombing was the first terrorist attack on a U.S. naval warship.

As with the 1998 Embassy attack, the strike on the *Cole* involved persistence and planning. Preparations for the attack began in 1998. As noted above, in January 2000, a group of plotters tried to attack another Navy warship. As with other terrorist attacks, several of the leading figures fled Yemen in the days before the bombing. Only the bombers themselves and several relatively poorly trained and unskilled radicals remained.

Peter Bergen, the author of *Holy War, Inc.* (Free Press, 2001) notes that Yemen had long been a hotbed of radical Islamist activity. Thousands of Yemenis volunteered to fight the Soviets in Afghanistan. Bin Ladin's first attack against the United States occurred against U.S. soldiers transiting Aden en route to Somalia in 1992. During the Yemeni civil war in 1994, the victorious northern regime employed Islamic radicals as shock troops in its attacks on the south. The State Department's 2000 *Patterns of Global Terrorism* indicates that Yemen was a safe haven for several terrorist groups, including the Egyptian Islamic Jihad – parts of which, after 1998, essentially had become in essence part of al-Qa'ida.

The Intelligence Community provided a steady stream of reporting indicating the danger of a terrorist attack in Yemen, but did not offer specific, actionable intelligence about the *U.S.S. Cole* attack itself. Other clues – while falling short of specific warning as to the time, place, and method of the attack – nevertheless offered considerable information regarding the need for force protection.

A post-attack CIA review, however, found that most of the information provided was quick-turnaround reporting, commentary, and analysis, with little historical context or long-term analysis. A senior DIA terrorism analyst noted in an interview that, in general, there was little effort to question underlying assumptions, such as preconceptions that Bin Ladin would not attack in Yemen because it was an important al-Qa'ida logistics hub or that al-Qa'ida would not strike a Navy ship because of the difficulty of doing so.

A separate inquiry by the Senate Select Committee on Intelligence (SSCI) also noted that although intelligence agencies "aggressively collected and promptly disseminated raw intelligence pertaining to terrorist threats," warning products lacked context and analytic depth.

The Challenge of Terrorism after the Cold War

The Joint Inquiry Staff review of the five incidents suggests several important characteristics of the emerging terrorist threat. Some were obvious to all at the time and others only became clear in retrospect, but all required changes in U.S. counterrorism efforts and the Intelligence Community more broadly. The characteristics include:

- The emergence of a new breed of terrorists practicing a new form of terrorism, different from the state-sponsored, limited-casualty terrorism of the 1960s, 1970s, and 1980s;

- International terrorists who operated in America and were willing to conduct attacks inside America;

- An adversary, al-Qa'ida, that is unusual in its dedication, size, organizational structure, and mission;

- The existence of a sanctuary in Afghanistan that allowed al-Qa'ida to organize, train, proselytize, recruit, raise funds, and grow into a worldwide menace; and

- Exploitation of permissive environments, such as Yemen, where governments were not willing or able to crack down on radical activity.

Table 1.0 provides an overview of these characteristics and notes which attacks suggest their presence.

Terrorism Characteristics	**WTC I/ Landmarks**	**Khobar Towers**	**African Embassy**	**Millennium Attacks**	***U.S.S. Cole***
Suggests new breed of terrorists seeking mass casualties emerging	X	X	X	X	
Operations in America	X			X	
Indicates al-Qa'ida and like-minded individuals are particularly dangerous adversaries	X		X	X	X
Terrorists exploit sanctuary in hostile country (Afghanistan or Iran)		X	X	X	X
Terrorists exploit governments unable or unwilling to crack down, including in the West	X		X	X	

Table 1.0. Characteristics of Terrorism Emerging from Past Attacks

A New Breed of Terrorism

Throughout the Cold War, radical left-wing groups or ethno-nationalist groups carried out most terrorist acts. The Palestine Liberation Organization, the Abu Nidal Organization, and the Japanese Red Army typified terrorist groups and their tactics. Moreover, many of these groups had state sponsors. Such groups shaped the U.S. government's conception of how a typical terrorist group behaved and the overall U.S. response to terrorism.

The first attack on the World Trade Center was an unambiguous indication that a new form of terrorism – motivated by religious fanaticism and seeking mass casualties – was emerging and focused on America. Interviews of FBI personnel who were involved in the 1993 investigation of that attack suggest their initial confusion as to the nature of their new adversary. Arabs from countries hostile to one another worked together. In

addition, they had no state sponsor – something that investigators had assumed they would eventually uncover.

Counterterrorism experts eventually recognized this change and incorporated it into their analysis. For example, a July 1995 National Intelligence Estimate noted a "new breed" of terrorist who did not have a sponsor, was loosely organized, favored an Islamic agenda, and had a penchant for violence. However, despite this recognition, neither the FBI nor the CIA assigned analysts and operators to focus exclusively on these individuals until January 1996.

An emphasis on mass casualties was another important change. Although attacks in the 1980s killed hundreds, no major terrorist group was attempting to kill thousands of civilians. However, a RAND Corporation study indicates that although the number of terrorist attacks decreased in the 1990s, overall casualties per attack increased. Terrorists proved able and willing to kill large numbers of people. This marked a significant change. Brian Jenkins, a foremost expert on terrorism, wrote in 1975 that: "[t]errorists want a lot of people watching and a lot of people listening and not a lot of people dead." Twenty years later, then-Director of Central Intelligence James Woolsey contended that: "[t]oday's terrorists don't want a seat at the table, they want to destroy the table and everyone sitting at it."

The increasing prevalence of religious terrorist organizations contributed directly to this shift. As Bruce Hoffman, a terrorism expert with the RAND Corporation, noted in a statement for the record for the Joint Inquiry: "[f]or the religious terrorist, violence first and foremost is a sacramental act or a divine duty." Ominously, al-Qa'ida began to incorporate suicide attackers – historically rare among Sunni terrorists – into its operations with the 1998 Embassy bombings.

This change in lethality was recognized early on within the Intelligence Community and by outside experts and communicated to U.S. government policy-makers. The DCI's December 1998 "declaration of war" on al-Qa'ida is only one indication of how seriously the danger of terrorism was taken within the Community. Policymakers from the Clinton and Bush administration have testified that the Intelligence Community repeatedly warned them of the danger al-Qa'ida posed and the urgency of the threat.

However, the strategic implications of this shift in lethality do not appear to have been fully recognized. Terrorism had gone from a nuisance that, though frightening and appalling, killed only hundreds , to a menace that directly threatened the lives of tens of thousands of Americans. Although many of the individuals working on the terrorism problem feared a mass casualty attack, the resources dedicated to the effort against al-Qa'ida remained limited or focused largely on force protection.

Operations in America

The first attack on the World Trade Center in 1993, five years before Bin Ladin openly called on his followers to bring *jihad* to America, was a painfully clear signal that Sunni extremists sought to kill Americans on American soil. Seven years later, the arrest of Ahmed Ressam should have dispelled any doubts that al-Qa'ida and its sympathizers sought to operate on U.S. soil, even though most of the masterminds remained overseas.

The United States itself was also an important location for terrorist logistics. For example, a conspirator in the 1998 Embassy bombings, Wadi el-Hage, a U.S. citizen who had served as Bin Ladin's personal secretary during Bin Ladin's time in Sudan and ran al-Qa'ida's Kenyan operations, lived in the United States over a year before he was arrested in August 1998. FBI agents and Kenyan police had hounded El-Hage from Kenya in August 1997, but he was able to settle in Texas.

Al-Qa'ida: An Unusual and Deadly Adversary

As the 1990s progressed, it became clear that al-Qa'ida was unusual, although not unique, in its skill, dedication, and ability to evolve. The 1993 World Trade Center attack and the plot against U.S. landmarks suggested a group of radical Islamic terrorists motivated who were highly motivated but not particularly skilled. The 1998 Embassy attack, the planned attack in Jordan around the Millennium, and the attack on U.S.S. Cole, in contrast, suggested an adversary that was highly capable. The 1993 plotters' ambition to kill thousands was frustrated because of limited organizational and financial backing. By the end of the decade, Sunni Islamic extremists had proven themselves highly skilled.

Al-Qa'ida operations before September 11 suggest several traits worthy of concern:

- Long-range planning. The Al-Qa'ida attack on the U.S. Embassies in Africa took five years from its inception. The planning for the attack on *U.S.S. Cole* took several years;

- Ability to conduct simultaneous operations. The Al-Qa'ida 1998 attack on U.S. Embassies in Africa and the Millennium plots demonstrate that al-Qa'ida was able to conduct simultaneous attacks, suggesting sophisticated overall planning. Hoffman notes that simultaneous terrorist attacks are rare, as few groups have enough skilled operators, logisticians, and planners;

- Emphasis on operational security. Al-Qa'ida's terrorist manuals and training emphasize that operations should be kept secret and details compartmented. Communications security is also stressed. Thus, disrupting these operations is difficult, even if low-level foot soldiers are arrested or make mistakes. Several al-Qa'ida attacks occurred with little warning. Even the successful disruption of part of a plot, as occurred during the Millennium, does not necessarily reveal other planned attacks, such as the planned attack on another U.S. Navy warship around the same time;

- Flexible command structure. As Hoffman notes, al-Qa'ida uses at least four different operational styles, including: a top-down approach employing highly-skilled radicals; training amateurs like Richard Reid, the so-called "shoebomber," to conduct simple, but lethal attacks; helping local groups with their own plans, as was done with the Jordanian plotters during the Millennium; and fostering like-minded insurgencies. The tactics that can stop one type of attack do not necessarily work against other plots.

- Imagination. Most terrorists are conservative in their methods, relying on small arms or simple explosives. The attack on U.S.S. Cole, however, was a clear indication of al-Qa'ida's tactical flexibility and willingness to go beyond traditional delivery means and targets.

Size also distinguishes al-Qa'ida from many terrorist groups. The recently disrupted Greek radical group, November 17, for example, contained fewer than 50 people. According to Hoffman, the Japanese Red Army and the Red Brigades both had fewer than 100 dedicated hard-core members. Even the Irish Republican Army, one of the most formidable terrorist organizations in the 1970s and 1980s, had no more than 400 activists. Arresting and prosecuting members of these groups was en effective way to end or lessen the threat they posed.

Although the number of highly skilled and dedicated individuals who have sworn fealty to Bin Ladin is probably in the low hundreds before September 11, the organization as a whole is much larger, with tens of thousands having gone through the training camps in Afghanistan. Its organizational and command structures, which employ many activists who are not formal members of the organization, make it difficult to determine where al-Qa'ida ends and other radical groups begin. Media reports indicate that al-Qa'ida has trained thousands of activists in Sudan and Afghanistan, and interviews of Intelligence officials indicate that al-Qa'ida can draw on thousands of supporters when raising funds, planning, and executing attacks.

The Problem of Sanctuary

The Joint Inquiry Staff review of the five attacks suggests a second characteristic that posed difficulties for the Intelligence Community and the U.S. government: terrorist exploitation of sanctuaries. Because of these sanctuaries, terrorist masterminds and leading operatives remained outside America's reach. In addition, terrorists could create an infrastructure of camps to train and recruit, allowing the groups to perpetuate and grow. Finally, terrorists exploited countries friendly -- or at least not hostile -- to the United States to plan operations and gain recruits, and even operate on U.S. soil with limited impunity.

Over many years, the United States worked with dozens of cooperating foreign governments to disrupt al-Qa'ida activities, arrest operatives, and otherwise prevent attacks, but Afghanistan itself was largely a haven. In its Afghan sanctuary, al-Qa'ida

built a network for planning attacks, training and vetting recruits, and indoctrinating potential radicals. In essence, al-Qa'ida created a terrorist army in Afghanistan with little interference. Intelligence successes such as the Millennium disruptions and arrests did little to affect this sanctuary.

Although the United States and its allies made numerous arrests following every major terrorist attack, Al-Qa'ida's senior leadership, including many of the masterminds for planning terrorist attacks, remained outside America's reach. The United States did eventually track down Ramzi Yusuf, the mastermind of the first World Trade Center attack, but several of those ultimately responsible for the Embassy bombings and *U.S.S. Cole* attack have thus far escaped justice.

The 1996 Khobar Towers attack, the 1998 African embassies attacks, and the 2000 *U.S.S. Cole* attack led the Departments of State and Defense to focus heavily on force protection, but not on meeting the challenge of Afghanistan, even though they recognized the dangers emanating from terrorist camps there. For example, the 2001 Department of Defense report on the *U.S.S. Cole* attack noted that the U.S. posture in general was too defensive and that "CENTCOM is essentially operating in the midst of a terrorism war."

Sanctuary for terrorists also took a less overt but more pernicious form in friendly countries. The Yemeni government, in contrast to the Taliban's Afghanistan, does not support Islamic radicalism, but terrorists exploited the country as a safe haven in planning the *Cole* attack due to Sanaa's unwillingness and at times inability to crack down. As became painfully clear after September 11, al-Qa'ida's network extends far beyond Afghanistan and the Middle East. London has long been a hub for Islamic radicals, and much of the planning for September 11 was done in Germany. Al-Qa'ida also raised money and recruited in Asia, Africa, and Europe – and in the United States. As Deputy Secretary of Defense Wolfowitz testified, "... even worse than the training camps [in Afghanistan] was the training that took place here in the United States and the planning that took place in Germany."

The Intelligence Community and concerned outside experts slowly became aware that effectively countering al-Qa'ida would require confronting the problem of terrorist sanctuary. In an interview, one Counterterrorism Center officer describes the problem of being unable to address the source and only seeing the manifestations as "trying to chop down a tree by picking the fruit." Similarly, other outside experts warned publicly of the problem of Afghanistan and called for action prior to September 11.

Steps Forward in the Fight Against Terrorism

As these challenges emerged, the Intelligence Community, and at times the U.S. Government, adopted several important measures that increased America's ability to fight terrorism in general and al-Qa'ida in particular. Many of these measures can only

be described obliquely or cannot be mentioned at all due to security strictures and rightful concerns about revealing intelligence methods.

Several counterterrorism efforts deserve mention:

- The early creation of a special unit to target Bin Ladin. Well before Bin Ladin became a household name – or even well-known to counterterrorist specialists – the CTC created a unit dedicated to learn more about Bin Ladin's activities. This unit quickly determined that Bin Ladin was more than a terrorist financier, and it became the U.S. Government's focal point for expertise on and operations against Bin Ladin. Later, after the 1998 Embassy attacks made the threat clearer, the FBI and the NSA increased their focus on al-Qa'ida and on Islamic extremism.

- Innovative legal strategies. In the trial of Shaykh Omar 'Abd al-Rahman, the Department of Justice creatively resurrected the civil war-era charge of "seditious conspiracy," enabling the U.S. Government to prosecute and jail individuals planning terrorist attacks in America.

- Aggressive renditions. Working with a wide array of foreign governments, the CIA helped deliver dozens of suspected terrorists to justice. These renditions often led to confessions and disrupted terrorist plots by shattering cells and removing key individuals.

- Improved use of foreign liaison services. As al-Qa'ida emerged, several CIA officials recognized that traditional U.S. intelligence techniques were of limited value in penetrating and countering the organization. They understood that foreign liaison could act as a tremendous force multiplier and tried to coordinate and streamline what had been an *ad hoc* process. In addition, the CIA and other Intelligence Community agencies strengthened their liaison relationships. Many al-Qa'ida cells around the world were disrupted as a result of this effort. Former National Security Adviser Berger has testified that cells were disrupted in about 20 countries after 1997.

- Strategic warning on the risk to U.S. interests overseas. After the bombings of U.S. embassies in Kenya and Tanzania in 1998, the CIA clearly and repeatedly provided warnings to senior U.S. policy makers, warnings that reached a crescendo in the summer of 2001. Policymakers from both the Clinton and Bush administrations have testified that the Intelligence Community repeatedly warned them that al-Qa'ida was both capable of and seeking to inflict mass casualties on America.

- Expansion of the FBI overseas. Director Louis Freeh greatly expanded the number of Legal Attache offices and focused them more on countries in which terrorism was prevalent or which were important partners against terrorism. By September 11, there were 44 legal attaché offices – up from 16 in 1992. Given the increasing role the FBI and the Department of Justice were playing in

counterterrorism, these offices helped ensure that domestic and overseas efforts were better coordinated. In addition, they provided the United States with additional access to foreign law enforcement entities, which were often taking the lead on counterterrorism.

- Augmenting the Joint Terrorism Task Forces (JTTFs). The Joint Terrorism Task Force model was originally created to improve coordination between the FBI and the New York Police Department. The first World Trade Center attack led to the expansion of the JTTFs to other cities and led to the inclusion of CIA officers in several task forces.

- Improved information sharing. Intelligence officials and policy makers took several measures to improve information sharing on terrorism among leading U.S. government agencies. The National Security Council revived the interagency process on terrorism and threat warning process, resulting in regular senior policy maker meetings concerning terrorism. The NSA and CIA held regular videoconferences among analysts after the 1998 Embassy bombings. Although many weaknesses remained, the FBI and CIA took steps to increase collaboration, which was extremely poor in the early 1990s, and established rotations in each other's counterterrorism units.

- Streamlined warning at the Defense Department. After the attack on *U.S.S. Cole,* the Department of Defense subordinated its terrorism analysis capability under the Joint Chief of Staff/Intelligence (J2), which has overall responsibility for warning in the Department of Defense. This reduced confusion and clarified responsibility for warning.

Problems And Steps Not Taken

Despite these measures to better fight terrorism, the Intelligence Community response was limited by a number of factors, including interpretations of U.S. law and overall U.S. counterterrorism policy. Among these factors were:

- Continued terrorist sanctuary. Up until September 11, al-Qa'ida raised an army in Afghanistan. In addition, it exploited the laxness of other countries' counterterrorism efforts (or the limits imposed by their legal systems).

- A "law enforcement" approach to terrorism. In part because options such as military force were not promising or deemed feasible, the United States defaulted to countering terrorism primarily through arrests and trials. The government's reliance on a law enforcement approach had several weaknesses, including allowing al-Qa'ida continued sanctuary in Afghanistan.

- Limited FBI aggressiveness at home. The FBI responded unevenly at home, with only some Field Offices devoting significant resources to Islamic extremists. An

overall assessment of the risk to America was not prepared, and much of the FBI's counterterrorism effort was concentrated abroad.

- Lack of a coordinated Intelligence Community response. The main intelligence agencies often did not collaborate. In particular, the absence of an effective system for "handoffs" between the FBI, the CIA, and NSA led to a gap in coverage with regard to international threats to the United States itself, an area that should have received particular attention.

- Difficulties in sharing law enforcement and intelligence information. The walls that had developed to separate intelligence and law enforcement often hindered efforts to investigate terrorist operations aggressively.

- Limited changes in intelligence priorities. Counterterrorism became an increasingly important concern for senior Intelligence Community officials, but collection and analytic efforts did not keep pace. Several issues competed with terrorism for attention, and priorities were often not clear.

Each of these factors is discussed in more detail below.

The Unsolved Problem of Sanctuary

Despite the Intelligence Community's growing recognition that Afghanistan was churning out thousands of radicals, there was little effort to integrate all the instruments of national power – diplomatic, intelligence, economic, and military – to address this problem. President Clinton declared after the 1998 bombing that "there will be no sanctuary for terrorists." The CIA and the FBI lacked the means to go after training camps in Afghanistan in a comprehensive manner, but little effort was made to utilize the U.S. military before September 11, with the notable exception of the August 20, 1998 cruise missile strikes.

Both the Clinton and Bush Administrations took some steps to address the problem of Afghanistan. Former National Security Adviser Berger has testified that after August 1998, "... the President authorized a series of overt and covert actions to get Bin Ladin and his top lieutenants." None of these actions appear to have hindered terrorist training or al-Qa'ida's ability to operate from Afghanistan. However, Berger also testified that there was little public or Congressional support for an invasion of Afghanistan before September 11, 2001.

Deputy Secretary of State Armitage and Deputy Secretary of Defense Wolfowitz have testified that, by the time of the September 11 attacks, the Bush Administration was far along in a policy review that called for a more aggressive policy against the Taliban and al-Qa'ida in Afghanistan. They were not, however, actively using the military against terrorism before this time.

The problem of permissive environments was understood before September 11, but little was done about it. As the National Commission on Terrorism (the "Bremer Commission") reported in 1998, "[s]ome countries use the rhetoric of counterterrorist cooperation but are unwilling to shoulder their responsibilities in practice, such as restricting the travel of terrorists through their territory ... ." The Commission explicitly mentioned Pakistan and Greece as friendly nations that presented difficulties in regard to terrorism. Although Congress in 1996 authorized the President to designate such countries as "not cooperating fully," this category was seldom applied.

Limited FBI Focus At Home

The FBI increased its focus on terrorism throughout the 1990s, but the Joint Inquiry Staff has found that it did not systematically and thoroughly make the changes necessary to fight terrorism in the United States. The FBI in 1999 made counterterrorism a separate division at headquarters. Changes in the field, however, were slower and less comprehensive.

This mixed record of attention contributed to the United States becoming, in effect, a sanctuary for radical terrorists. As General Brent Scowcroft has testified, "the safest place in the world for a terrorist to be is inside the United States ... as long as they don't do something that trips them up against our laws, they can do pretty much all they want."

Several observations, taken together, provide support for this contention:

- The leading NSC-level U.S. policy maker with counterterrorism responsibilities contends that, with the exception of the New York Field Office, the FBI field offices around the country were "clueless" with regard to counter-terrorism and al-Qa'ida and did not make them priorities. Former National Security Advisor Berger has testified that the FBI was not sufficiently focused on counterterrorism before September 11.

- FBI officials working on terrorism faced competing priorities, and their ranks were not augmented. Only one FBI analyst worked strategic analysis exclusively on al-Qa'ida before September 11. The former Chief of the FBI's International Terrorism Section states that he had more than 100 fewer Special Agents working on international terrorism on September 11 than he did in August 1998.

- In the New York Field Office, the office of origin for all major Bin Ladin-related investigations, attention and effort focused primarily on investigating overseas attacks.

- According to FBI officers, FBI training on counterrorism was extremely limited, only increasing after September 11.

- Scowcroft, in testimony to the Joint Committee on September 19, contended that the best FBI agents worked criminal cases, not counterterrorism not linked to traditional criminal work. Dale Watson, former Executive Assistant Director for Counterterrorism and Counterintelligence strongly disagreed with this characterization.

- The FBI did not press the CIA or other intelligence agencies such as NSA for information that might have led to more FBI leads at home.

- An FBI agent with considerable counterterrorism experience noted that foreign governments often knew more about radical Islamist activity in the United States than did the U.S. Government because these governments saw this activity as a threat to their own power.

The FBI was not able to gather intelligence from disparate cases nationwide to produce an overall assessment of al-Qa'ida's presence in the United States. The FBI's decentralized structure contributed to the Bureau's inability to correlate the knowledge its components possessed. In addition, the FBI's case-based approach led the terrorist threat to be viewed through a narrow lens.

Attention to terrorist activity in the United States often increased after an attack when the links between radicals in the United States and overseas became better known. For example, Watson says that he only knew of three al-Qa'ida suspects in the United States before the 1998 Africa Embassy bombings, but some 200 FBI counterterrorism cases were opened after the bombing.

FBI officials argue, however, that al-Qa'ida proved a difficult target in the United States. Director Freeh notes that al-Qa'ida operations were small and were not connected to real "cells" – a judgment echoed by several senior FBI investigators. These investigators claim that "international radical fundamentalists" operate in the United States but that real al-Qa'ida members – those involved in planning or carrying out attacks -- avoid other radicals and stay clear of radical mosques as part of their tradecraft.

Joint Inquiry Staff investigators received mixed reports on the FBI's aggressiveness in penetrating radical Islamic groups in the United States. Sources proved invaluable in the successful prevention of the 1993 attack on New York landmarks and for the prosecution of the first World Trade Center attack. In addition, the FBI had numerous wiretaps and several human informants in its effort to target various radical Islamist organizations. However, an FBI official involved in the investigations of the first World Trade Center attack and other terrorist plots notes that the Bureau made it exceptionally difficult to handle sources (as opposed to working with cooperating witnesses), a difficulty that increased in the 1990s. The agent contends that the FBI did not want to be associated with persons engaged in questionable activities, even though they can provide solid information. In addition, he advised that individual agent performance ratings downgraded the importance of developing informants.

The FBI also did not inform policy makers of the extent of terrorist activity in the United States. Former National Security Advisor Berger has testified that the FBI assured him that there was little radical activity in the United States and that this activity was "fully covered." Although the FBI conducted many investigations, senior FBI officials and analysts did not accumulate these pieces into a larger picture.

The FBI's limited attention to the danger at home reflects a huge gap in the U.S. Government's counterterrorism structure: a lack of focus on how an international terrorist group might target the United States itself. No agency appears to have been responsible for regularly assessing the threat to the homeland. In his testimony before the Joint Committee on September 19, Deputy Secretary of Defense Wolfowitz asserted that an attack on the United States fell between the cracks in the U.S. Intelligence Community's division of labor. He noted that "... there is a problem of where responsibility is assigned." The CIA and the NSA followed events overseas, and their employees saw their job as passing relevant threat information to the FBI. The FBI, on the other hand, does not have the analytic capacity to prepare assessments of U.S. vulnerability and relies heavily on the CIA for much of its analysis.

In addition, prior to September 11, FBI Field Offices usually did not initiate investigations on individuals believed to be permanently outside of the United States. There were no legal barriers that prevented such an investigation, but one FBI field agent claimed that FBI Headquarters discouraged such investigations. In such cases, it was within the discretion of the case agent whether to inform the CIA, Immigration and Naturalization Service, State Department, or other agencies about the agent's investigative interest. As a result, the agent told the Joint Inquiry Staff that the FBI often did not learn when suspects returned to the United States.

Law Enforcement: A Problematic Approach to Counterterrorism

The perpetrators of the 1993 World Trade Center plot and the attack on New York landmarks, and several of those involved in the 1998 Embassy bombing, as well as other plots were all prosecuted. This emphasis on prosecution continues a trend begun in the 1980s, when Congress and President Reagan gave the FBI an important role in countering international terrorism, including events overseas.

U.S. Government officials apparently never intended to rely exclusively on law enforcement to fight terrorism. By default, however, law enforcement tools became the primary instrument of American counterterrorism strategy. Senior Department of Justice officials including Mary Jo White, who as U.S. Attorney in the Southern District of New York prosecuted most of the most important cases against al-Qa'ida, point out that they saw their efforts as an adjunct to other means of fighting terrorism.

In addition, the law was often used to disrupt the activities of suspect terrorists in the United States. If appropriate, U.S. Attorney offices prosecuted individuals for perjury, passport fraud, and other crimes in an effort to splinter the broader terrorism

support network. White favored using the law against individuals for "spitting on the sidewalk"-type of crimes if they were suspected terrorists.

Prosecutions do have several advantages in the fight against terrorism. As White noted, prosecutions take terrorists off the street. She acknowledges that this does not shut down an entire group, but some bombs do not go off as a result of the arrests. In addition, critical intelligence often comes from the investigative process, as individual terrorists confess or reveal associates through their personal effects and communications. As former FBI Director Louis Freeh pointed out, "you can't divorce arrest from prevention." White also contends that the prosecutions may deter some, though not all, individuals from using violence. Finally, the threat of a jail sentence often induces terrorists to cooperate with investigators and provide information.

Heavy reliance on law enforcement, however, also has costs. As Pillar notes, it is easier to arrest underlings than masterminds. Those who organize and plan attacks, particularly the ultimate decision makers who authorize them, are often thousands of miles away when an attack is carried out. In addition, the deterrent effect of imprisonment is often minimal, particularly for highly motivated terrorists such as those in al-Qa'ida. Moreover, law enforcement is time-consuming. The CIA and the FBI expended considerable resources supporting investigations in Africa and in Yemen regarding the Embassies and *U.S.S. Cole* attacks, a drain on scarce manpower and resources that could have been used to gather information and disrupt future attacks. Finally, law enforcement standards of evidence are high: making a case that meets these standards often requires unattainable intelligence and compromises sensitive sources or methods.

At times, law enforcement and intelligence have competing interests. The former head of the FBI's international terrorism division notes that Attorney General Reno leaned toward closing down FISA surveillance if they hindered criminal cases. White, however, notes that the need for intelligence was balanced with the effort to arrest and prosecute terrorists. In addition, as noted earlier, convictions that help disrupt terrorists are often on minor charges (such as immigration violations), which do not always convince Field Office personnel that the effort is worthwhile compared with putting criminals in jail for many years. As former FBI Executive Assistant Director for Counterterrorism and Counterintelligence Dale Watson explains, Special Agents in Charge of FBI Field Offices focused more on convicting than on disrupting.

The reliance on law enforcement when individuals have fled to a hostile country such as Iran or the Taliban's Afghanistan appears particularly ineffective, as the masterminds are often beyond the reach of justice. One FBI agent scorns the idea of using the Bureau to take the lead in countering al-Qa'ida, noting that all the FBI can do is arrest and prosecute. They cannot shut down training camps in hostile countries. He notes that, "[it] is like telling the FBI after Pearl Harbor, 'go to Tokyo and arrest the Emperor.'" In his opinion, a military solution was necessary because, "[t]he Southern District doesn't have any cruise missiles."

Before September 11, the United States did not regularly use military force against terrorists. However, senior policy makers have suggested that the policy community did not see a sustained military campaign against terrorist infrastructure in Afghanistan as politically feasible. Moreover, the U.S. military reportedly did not believe it should take the lead on counterterrorism before September 11.

Lack of a Coordinated Intelligence Community Response

Counterterrorism, like other transnational threats such as drug trafficking, requires close coordination among domestically and internationally focused intelligence agencies. However, each of the principal collectors of counterterrorism intelligence – the FBI, the CIA, and the NSA – has distinct missions, distinct sets of legal authorities and restraints, and distinct cultures that can hinder collaboration. Throughout the Cold War, it was acceptable to divide responsibilities depending on whether a threat was abroad or located in the United States. Indeed, repercussions from the collaboration between the three agencies against perceived domestic security threats associated with anti-Vietnam War protests in the 1960s and 1970s reinforced the importance of this division of responsibility.

As the 1990s progressed, coordination in general improved as the different agencies became aware of each other's requirements and limits. For example, in one late 1990s operation, information was obtained through intelligence channels and could not be used in a criminal prosecution because the chain of custody did not involve U.S. law enforcement officials. However, by 2001 greater cooperation between intelligence and law enforcement agencies better addressed such issues.

Despite several such positive steps, there was only a limited effort to act in a unified manner – as a Community, rather than as a loose collection of distinct agencies. Even after the 1993 World Trade Center attack, the Millennium plot, and links to the United States in the 1998 Embassy attacks revealed that Islamic extremists had a global network that included the United States, there does not appear to have been any significant sustained attempt by the FBI, the NSA, and the CIA to work together to collect information about the contacts between foreign persons in the United States and foreigners abroad.

Several problems noted in interviews suggest a lack of integration:

- Not all JTTFs included CIA officers, hindering a thorough and smooth dissemination of information among international, national, and local agencies with counterterrorism responsibilities. Of the 35 JTTFs active on September 11, only six had CIA officers on them.

- At times, agencies did not disseminate information due to a lack of recognition of its value to other parts of the Intelligence Community. Details and fragments from communications, operations officers, FBI investigators, and others often were not passed on. This was not, in general, due to "turf"

issues or a deliberate intention to hinder counterterrorism, but rather due to a failure to recognize that this information was wanted.

- Information was often shared among institutions but did not necessarily flow to those who most needed it.

- Poor information systems and the high level of classification, prevented FBI field officers from using NSA and CIA data.

- Senior management often appears unaware of information sharing problems. Former FBI Director Louis Freeh state that all intelligence was provided to the CIA and that there was no problem with the amount of such information or the level at which this transfer of information was taking place, an assertion that individuals at the working level at the CIA strongly contest; and

- When investigating radicals in the United States, the FBI faces legal and regulatory restrictions (discussed further below) on the dissemination of information to intelligence agencies obtained in the course of FBI investigations in the United States.

An unclear division of labor also appears to have hindered collaboration. NSA officials contend that the responsibility for collecting information concerning foreign radicals in the United States was the responsibility of the FBI. NSA officials maintain that this was true even when these individuals were communicating internationally. As a result, NSA did not use one sensitive collection technique that would have improved its chances of successful collection. NSA adopted this strategy even though its mission includes the collection and exploitation of foreign communications that have one communicant in the United States (and such coverage would have been allowed under a FISA). NSA does not appear to have developed a plan with the FBI to ensure that the Bureau would routinely pursue collection in cases where the NSA would not do so.

Even the CTC, the Intelligence Community's counterterrorism organization that was expressly designed to foster a Community-wide response, suffered from parochialism. The creation in 1986 of the DCI's Counterterrorist Center was a vital step in the United States effort against terrorism. Fifteen years after its creation, it had grown and integrated other parts of the Intelligence Community, including the FBI and NSA. Rotations to the CTC from other Agencies helped improve cooperation, as did a growing recognition of the value of different forms of reporting. Yet the CTC still remained largely a CIA organization closely tied to the Directorate of Operations. The Center's location at the CIA reinforced this perception. Interviews at the NSA, DIA, and FBI indicate that many officials there saw the CTC primarily as a CIA rather than a community organization. It was not clear whether rotational personnel from other agencies were meant to perform duties of CTC officers, act solely as liaison with their home agencies, or do both. As a result, the CTC did not always lead the Intelligence Community as a whole or foster collaboration.

The net effect of these problems was gaps in the collection and analysis of information about individuals and groups operating both in the United States and abroad. The actions of those responsible for the attacks of September 11 demonstrate why effective integration of domestic and foreign collection is critical in understanding fully the operations of international terrorists. We now know that several hijackers communicated extensively abroad after arriving in the United States and at least two entered, left, and returned to the United States. Effective tracking of their activities, which would have required coordination among the agencies, might have provided important additional information.

Priorities Often Not Updated

Starting in 1995, the Intelligence Community's strategic-level guidance for national security priorities was set by Presidential Decision Directive (PDD)-35. In an attempt to rank the myriad of post-Cold War threats facing the United States, PDD-35 established a tier system. Unfortunately, the tiers were broad and overly concentrated at the upper levels (e.g., there were both Tier 1A and Tier 1B priorities). Moreover, PDD 35 was never amended despite language that required an annual review. As certain threats, including terrorism, increased in the late 1990s, none of the "lower level" Tier 1 priorities were down-graded so that resources (money and people) could be reallocated. To much of the Intelligence Community, everything was a priority – the U.S. wanted to know everything about everything all the time.

The vagueness of PDD-35 quickly translated into an overburdened requirements system within the Intelligence Community. For example, NSA analysts acknowledged that they had far too many broad requirements (some 1,500 formal ones) that covered virtually every situation and target. Within these 1,500 formal requirements, there were almost 200,000 "Essential Elements of Information" (EEI) that were mandated by customers. Analysts understood the gross priorities and worked the requirements that were practicable on any given day. However, several have acknowledged that, in some cases, the priority demands precluded them from delving deeply into certain areas.

The Wall

Previous Staff Statements have described a variety of situations in which significant information was not shared between personnel from different Intelligence Community agencies, or between the agencies themselves, or between those agencies and organizations outside the Intelligence Community. While some of these episodes may be traced to the press of business and the fast pace of counter terrorism operations, most have been described to the Joint Inquiry Staff in terms that relate to the many "walls" that have been built between the agencies over the past sixty years as a result of a variety of legal, policy, institutional, and individual factors. Several prominent commissions, including those led by Ambassador Bremer and Governor Gilmore, have noted the difficulties caused by the Wall and called on the Attorney General to minimize problems whenever possible by clarifying procedures and expediting information sharing.

The walls in question include those that separated foreign activities from domestic activities, foreign intelligence operations from law enforcement operations, the FBI from the CIA, communications intelligence from other types of intelligence, Intelligence Community agencies from other federal agencies, classified national security information from other forms of evidentiary information, and information derived from electronic surveillance for foreign intelligence or criminal purposes from those who are not directly involved in its collection. A brief summary of the sources and substance of several of these walls is necessary to understand the difficulties they have caused and the nature of any effort to alter them.

Following the end of World War II, the National Security Act of 1947 created the United States' first peacetime civilian intelligence organization, the Central Intelligence Agency. Two fundamental considerations shaped that act: that the United States not enable a Gestapo-like organization that coupled foreign intelligence and domestic intelligence functions; and that the domestic jurisdiction of the Federal Bureau of Investigation be preserved. In order to satisfy these two considerations, the Act provided that the CIA should have no police, subpoena, or law enforcement powers, and should not perform any internal security functions.

Generations of intelligence professionals have been trained in this distinction, the doctrine of disclosing information only to those who have a demonstrable "need to know," and the rigidities of the national security classification system. On the law enforcement side, it has long been recognized that confidentiality, protection of witnesses, and secrecy of grand jury information are essential to the successful investigation and prosecution of crimes. Thus, to both the law enforcement and foreign intelligence professions, proper security practices and strict limits on the sharing of information are second nature.

By the mid-1970s, however, the law enforcement interest in disclosing evidence to prosecute and convict gradually came to prevail over the foreign intelligence interest in maintaining secrets. This most often occurred in the context of an espionage investigation where the mutual interest in successful prosecution would force the two sides to come together temporarily, often with great friction, and craft special procedures to limit the exposure of intelligence information in the case, but yet produce sufficient evidence to convict the defendant. This culminated in the Classified Information Procedures Act of 1980 that established a statutory framework for the use and protection of classified information in criminal proceedings.

Most of the day-to-day differences in practice and procedure were cloaked from public discussion because of the need for confidentiality on the one hand and secrecy on the other. However, the foreign intelligence/law enforcement division of authority, activity, and access over this thirty–year period are best illustrated by the development of separate paths for law enforcement- and foreign intelligence-related electronic surveillance and searches, an area where Constitutional and jurisprudential factors require a firm public legal basis.

The Fourth Amendment to the Constitution requires a judicial warrant for most physical searches for law enforcement purposes. In 1967, the Supreme Court decided that law enforcement officers engaged in electronic surveillance for criminal investigative purposes also should be required by the Constitution to obtain a warrant based upon probable cause to believe

a crime is being committed. Congress established such standards for obtaining such judicial warrants in 1968.

That 1967 Supreme Court decision expressly reserved the question of whether electronic surveillance for foreign intelligence purposes also required a warrant from a judge. A Supreme Court case in 1972 drew the limits of this practice by holding that the activities of a domestic group could not be subjected to warrantless electronic surveillance authorized by the President or Attorney General unless the executive branch could establish a connection between the group and a foreign power. The Government's assertion that such surveillance was necessary in order to collect intelligence about the group as part of an "internal security" or "domestic security" investigation was not sufficient to override the Constitutional requirement for a warrant. The Court did not address "the scope of the President's surveillance power with respect to the activities of foreign powers within or without he country."

A few years later, Congress conducted extensive investigations into the activities of the U. S. intelligence agencies. These activities included warrantless electronic surveillance of U. S. citizens who were not agents of any foreign power and warrantless physical searches within the United States conducted in the name of protecting intelligence sources and methods. Based on these findings and the Supreme Court's 1972 suggestion, Congress and the Executive branch agreed on the enactment of the Foreign Intelligence Surveillance Act in 1978.

The FISA established a special court that was designed to meet the various points the Government had relied upon in the past to argue that the courts were not equipped to authorize foreign intelligence-related surveillances. Also, instead of probable cause to believe a crime is being committed, the Act required the Government to demonstrate probable cause that the target is a foreign power or agent of a foreign power and is engaged in clandestine intelligence activities or international terrorism and, where the target is a U. S. person, that the person's activities involve or may involve a violation of U. S. criminal laws. Recognizing that intelligence and law enforcement interests would coincide in many cases where foreign intelligence surveillance is appropriate, such as espionage and terrorism investigations, the Act permits information produced by the surveillance to be shared with law enforcement personnel. It also provides procedures by which such information may be tested and used in prosecutions. However, to ensure that the division between foreign intelligence- and law enforcement-related electronic surveillance was maintained, the Act required a certification that "the purpose" of a proposed FISA surveillance be the collection of foreign intelligence information.

As the 1980s began, the law enforcement and intelligence communities worked together most often in the context of counterintelligence investigations and counternarcotics programs. The law enforcement agencies became more acutely aware in the course of this collaboration of the evidentiary complications that could arise as a result of using intelligence in their law enforcement efforts. For example, defense attorneys pursuing discovery of all investigative information relating to the guilt or innocence of their clients could move to have charges dismissed if information was withheld by the Government on the basis of national security classification.

This increased interaction also required that the intelligence agencies devise creative ways to disseminate intelligence for law enforcement use while protecting intelligence sources and methods. Intelligence agencies began reporting information in special formats (i.e., "tear lines") to allow less classified or unclassified versions of intelligence to be separated from the more highly classified portions and shared with law enforcement personnel. They also provided intelligence information in classified form to law enforcement organizations "for lead purposes only" so as to allow law enforcement organizations to take action on the information while preventing it from becoming entwined in criminal investigations.

In addition, individuals in the Justice Department and United States Attorneys' Offices began to be designated as focal points for intelligence reporting. These officials were given the responsibility of insulating law enforcement and prosecutive personnel from intelligence information and finding ways to allow them to benefit from it without incorporating it into their case files. These arrangements began to be generically referred to as "walls."

An additional form of "wall" was developing at the Department of Justice in connection with FISA electronic surveillances and physical searches for intelligence purposes. In order to avoid courts ruling that FISA surveillances were illegal because foreign intelligence was not their "primary purpose," DOJ lawyers began to limit contacts between FBI personnel involved in these activities and FBI and DOJ personnel involved in criminal investigations.

The Attorney General issued special procedures in 1995 regulating such contacts in FBI foreign intelligence investigations where FISA was being used and potential criminal activity was discovered. These procedures required three-way notice and coordination between the FBI, DOJ's Criminal Division and DOJ's Office of Intelligence Policy and Review (OIPR). These procedures were augmented by the Attorney General in 2000 and 2001 and were actually adopted and incorporated by the FISA Court in FISA surveillances that it approved after November 2001.

The wall in FISA matters became thicker and higher over time, as is explained in the May 17, 2002 opinion of the FISA Court rejecting proposed changes in the procedure by the Attorney General:

> . . . . to preserve . . . the appearance and the fact that FISA [was] not being used *sub rosa* for criminal investigations, the Court routinely approved the use of information screening "walls" proposed by the government in its applications. Under the normal "wall" procedures, where there were separate intelligence and criminal investigations, or a single counter-espionage investigation with overlapping intelligence and criminal interests, FBI criminal investigators and [DOJ] prosecutors were not allowed to review all of the raw FISA [information] lest they become *de facto* partners in the FISA [operations]. Instead, a screening mechanism, or person, usually the chief legal counsel in an FBI field office, or an assistant U. S. attorney not involved in the overlapping criminal investigation, would review all of the raw [information] and pass on only that information which might be relevant evidence. In unusual cases . . . , [DOJ] lawyers in OIPR acted as the "wall." In significant cases, . . . such as the bombings of the U. S. embassies in Africa, . . . where criminal investigations of FISA targets were being

conducted concurrently, and prosecution was likely, this Court became the "wall" so that FISA information could not be disseminated to criminal prosecutors without the Court's approval.

The resulting thicket of procedures, reviews and certifications regarding whether there had been any sharing of FISA information or contact between foreign intelligence and criminal investigators was bound to lead to confusion and error. The Department of Justice in March 2000 identified substantial errors in the factual applications that were being presented to the FISA Court. By September 2000, the Department of Justice identified errors in about 75 FISA matters, and the Court was advised of an additional group of erroneous filings in March 2001. In response, the FISA Court decided not to accept even unknowingly erroneous affidavits from FBI agents; all DOJ personnel involved in FISA matters were required to certify to their understanding that no information could be shared with criminal prosecutors without the Court's approval; one FBI agent was barred from being involved in matters before the FISA Court and is subject to an internal investigation; and a large number of FISA surveillances – including many that related to international terrorism – expired in the spring and summer of 2001 while the underlying applications were being reviewed and corrected.

The consequences of the FISA Court's approach to the Wall between intelligence gathering and law enforcement prior to September 11 were extensive. FBI personnel feared suffering the same fate as the agent who had been barred. FBI personnel who were involved in FISA matters began to avoid even the most pedestrian contacts with the criminal side of the FBI or DOJ since such contacts could result in intensive scrutiny by OIPR and the FISA Court. NSA, unable to be certain that it could identify which of its reporting came from FISA authorizations and which did not, began to indicate on all its reporting that the content could not be shared with law enforcement personnel without the prior approval of the FISA Court. In addition, field agents complained that getting a FISA approved was time-consuming.

The various types of walls have had other consequences as well, including specific examples of direct relevance to this inquiry. For example, a CIA employee advised two FBI employees in January 2000 regarding what the CIA knew about the activities of future hijacker Khalid al-Mihdhar in Malaysia, but not the fact that al-Mihdhar had a multiple entry U. S. visa. The CIA officer stated in an e-mail at the time that the FBI would be brought "into the loop" immediately as soon as "something concrete" was developed "leading us to the criminal arena or to known FBI cases." Perhaps reflecting the deadening effect of the long standing wall between CIA and FBI, the FBI agents reportedly thanked the CIA employee and "stated that this was a fine approach" even though the FISA wall did not apply in this case.

Even in late August 2001, when the CIA advised the FBI, State Department, INS, and Customs that al-Mihdhar, al-Hazmi, and two other "Bin Laden-related individuals" were in the United States, FBI headquarters refused to accede to the New York field office's recommendation that a criminal investigation be opened, which would allow greater resources to be dedicated to the search for al-Mihdhar. This was based on the reluctance of FBI headquarters to utilize intelligence information to draw the connection between al-Mihdhar and *U.S.S. Cole* bombing that would be necessary for a criminal investigation. FBI headquarters lawyers took the position that criminal investigators "CAN NOT" be involved and that any substantial

criminal information that might be discovered would be "passed over the wall" according to proper procedures. Again, the FBI apparently applied the FISA "wall" procedures to a non-FISA case.

When the FBI contacted INS and the State Department's Diplomatic Security Bureau to seek visa information regarding al-Mihdhar and al-Hazmi, the Bureau did not share with the other organizations the intelligence information that was the basis for the request. Both the INS and the State Department say they would have been able to bring their informational and personnel resources to bear with greater chances of success if they had been told the emergency nature of the search.

The USA PATRIOT Act provided unambiguous authority for the Attorney General and other law enforcement officials to disclose to the Director of Central Intelligence any foreign intelligence collected in the course of a criminal investigation. The Act also amended the requirement that intelligence be "the purpose" of a FISA search. Since Congress emended FISA, the FISA Court rejected DOJ rules that would have allowed the Criminal Division to direct or control FISA cases – the DOJ has appealed that ruling. This was intended to reduce, if not remove altogether, the wall that has grown up around FISA operations. The USA PATRIOT Act also amended the Rules of Criminal procedure to allow foreign intelligence developed in grand jury proceedings to be shared with non-law enforcement personnel. Another amendment permits information from law enforcement electronic surveillances to be shared with non-law enforcement personnel

These changes to the law, and the shock of September 11 itself, have had some beneficial impacts on the ability and willingness of the Intelligence agencies and their personnel to share information with one another and with non-Intelligence Community agencies and personnel. Whether and to what extent this impact can be sustained remains to be seen.

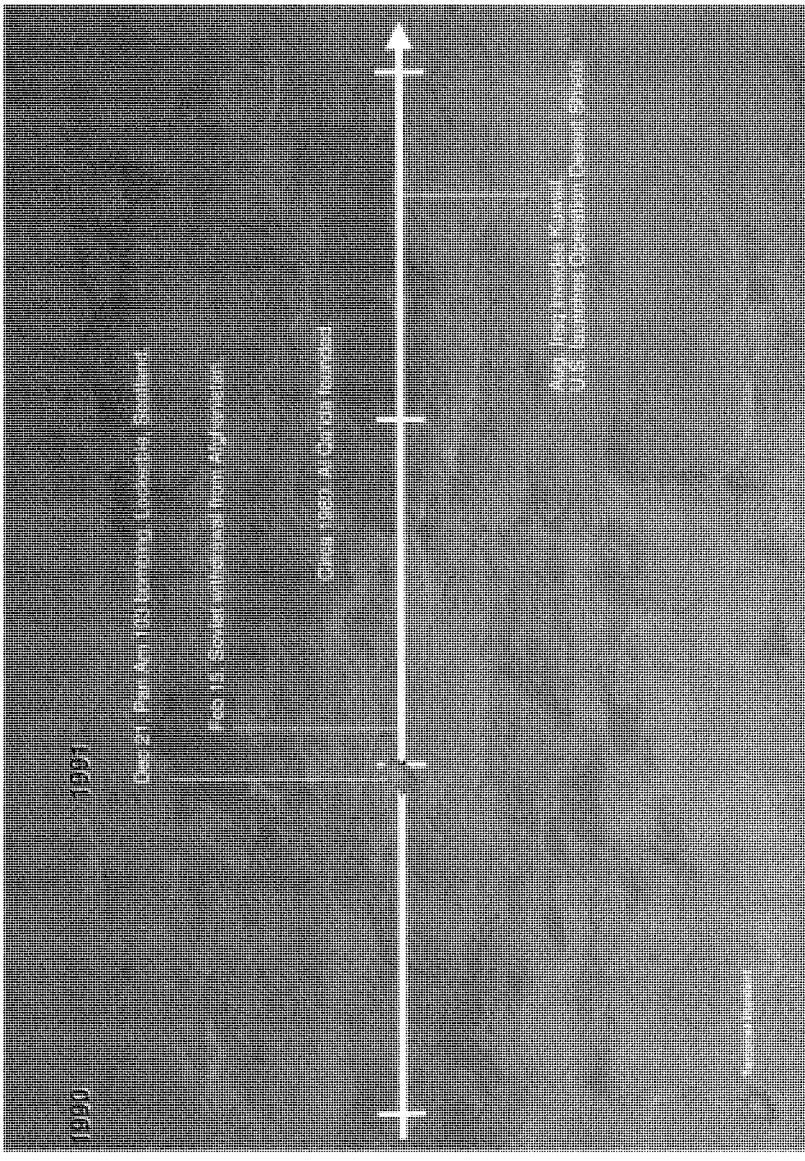
Final Words

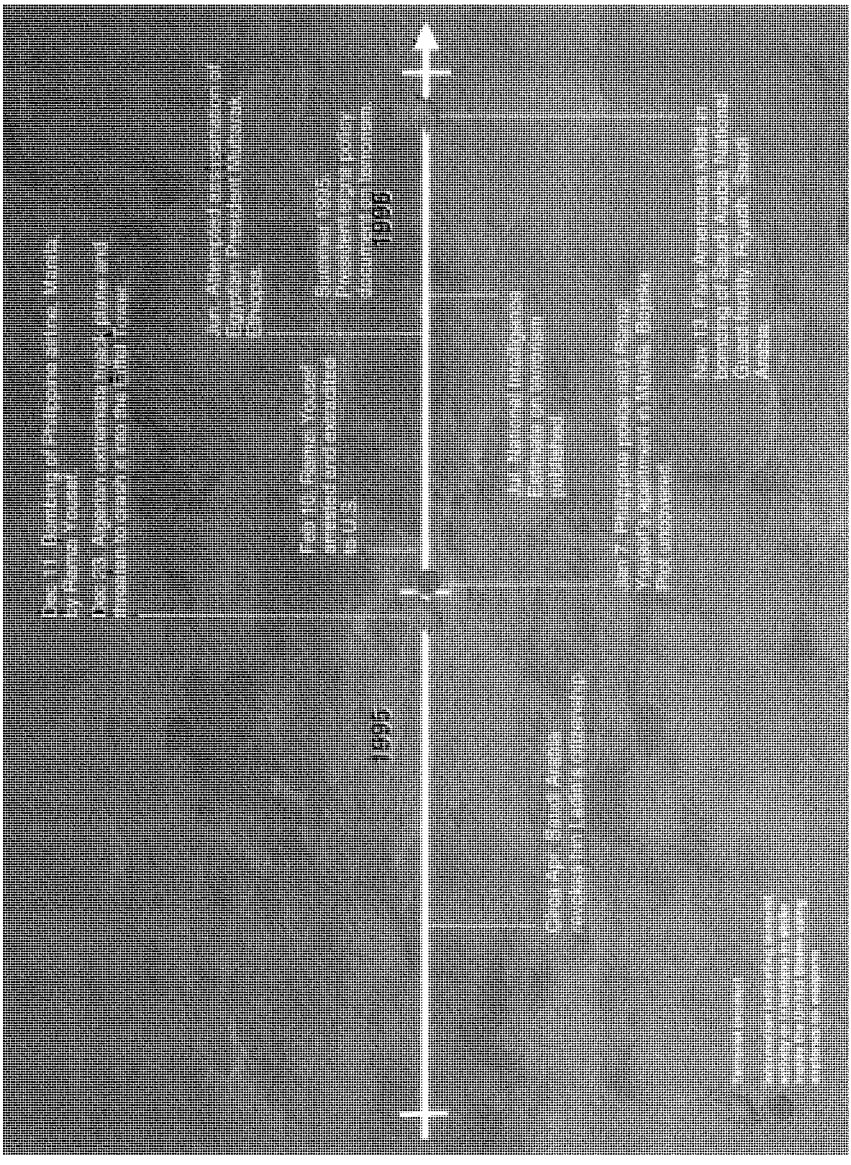
As this review suggests, the Intelligence Community made several impressive advances in fighting terrorism since the end of the Cold War, but many fundamental steps were not taken. Individual components of the Community scored impressive successes or strengthened their effort against terrorism, but important gaps remained. These included many problems outside the control or responsibility of the Intelligence Community, such as the sanctuary terrorists enjoyed in Afghanistan and legal limits on information sharing between intelligence and law enforcement officials.

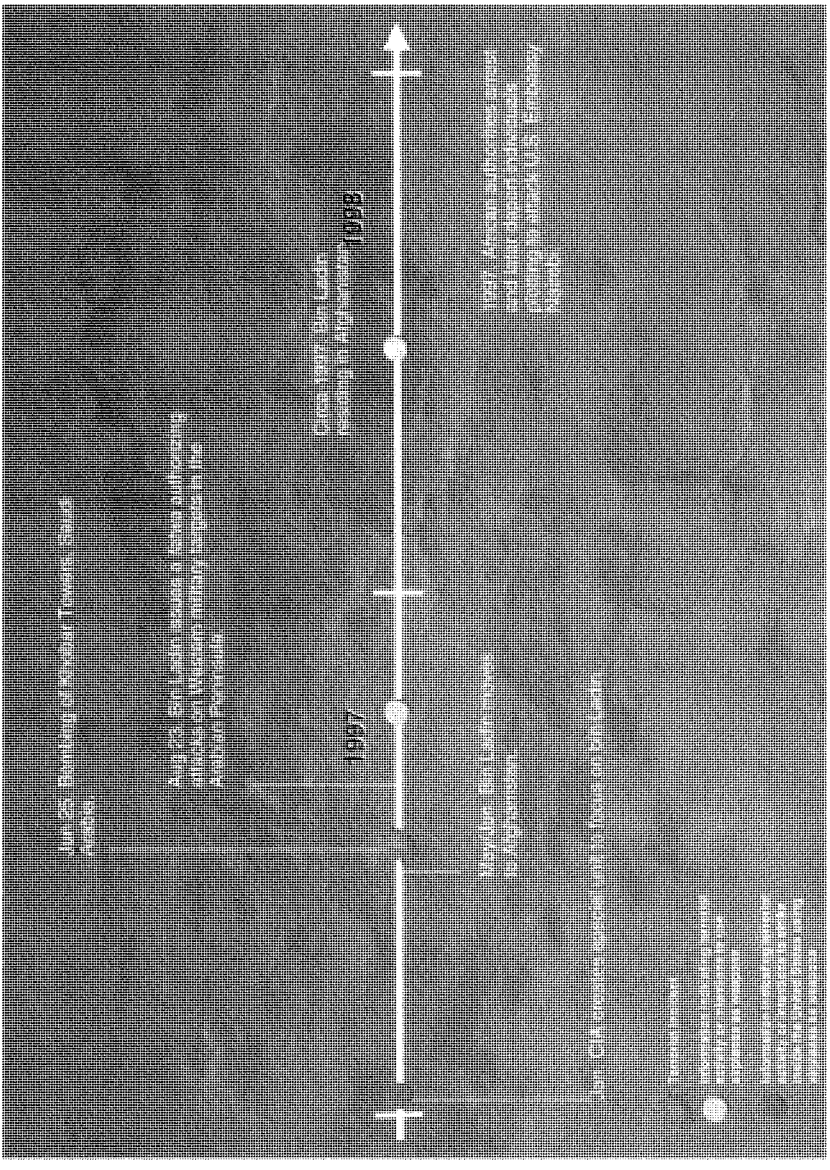
However, another major contributing factor was that the Intelligence Community did not fully learn the lessons of past attacks. On September 11, 2001 al-Qa'ida was able to exploit the gaps in the U.S. counterterrorism structure, some of which were remeditable, to carry out its devastating attacks.

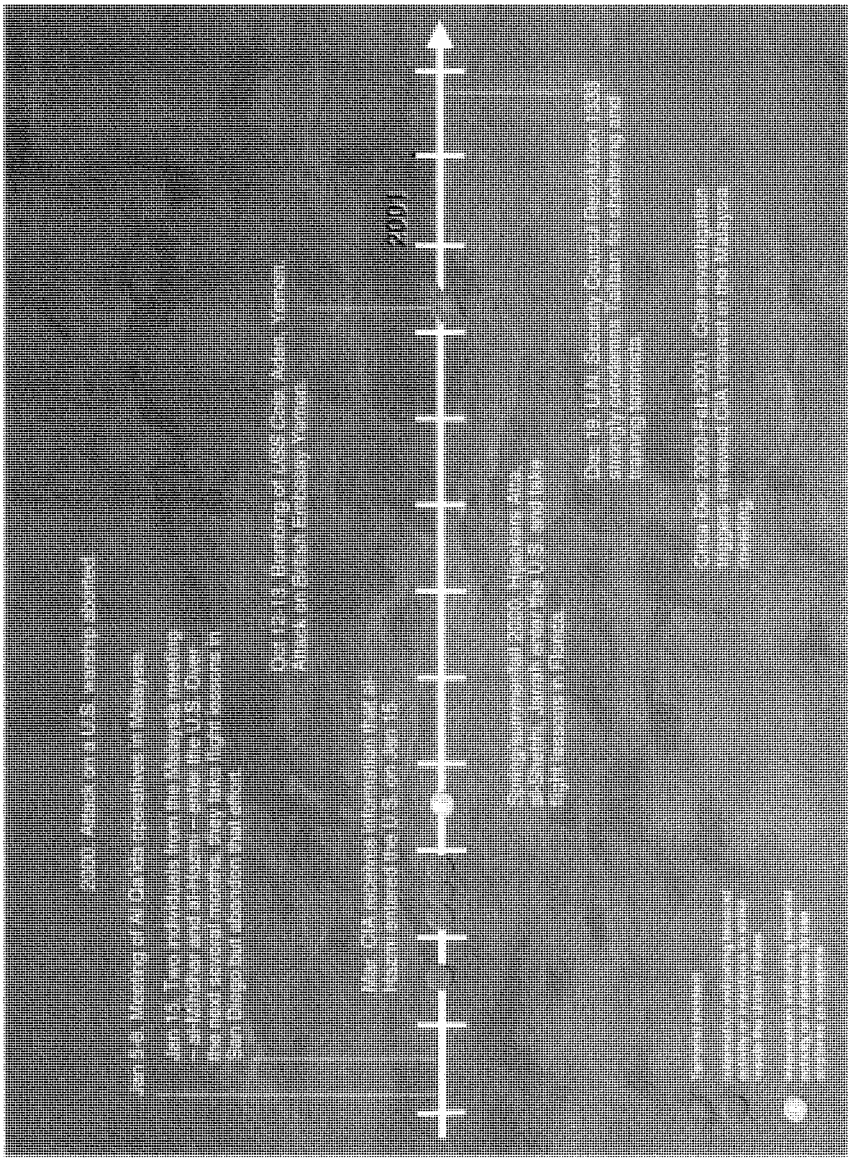
Selected Events in the
Chronology of Terrorism,
1982–2001

1982
1983
1984
1985
Pan-Asian Wars
Indochina War
Pan-Arab Wars
Arab-Israeli War
Iran-Iraq War
Gulf War
Afghanistan War
Iraq War









TESTIMONY OF ELEANOR HILL, STAFF DIRECTOR, JOINT INQUIRY COMMITTEE

Ms. HILL. Mr. Chairman, members of the two committees, good morning.

The purpose of today's hearings is to review past terrorist attacks, both successful and unsuccessful, by al-Qa'ida and by other groups against the United States. This review focuses not only on the attacks themselves, but also on how the Intelligence Community changed its posture in response and on broader themes that demand close scrutiny by the committees.

This review of past attacks and issues is not as deep or as thorough as our inquiry into the events of September 11. Instead, it represents a more general assessment of how well the Community has adapted to the post-Cold War world, using counterterrorism as a vehicle.

In conjunction with our work regarding the September 11 attacks, the staff has reviewed documents related to past terrorist attacks and interviewed a broad range of individuals involved in counterterrorism throughout the last decade. The documents include formal and informal lessons learned, studies undertaken by different components of the Community and the U.S. military, briefings and reports prepared by individuals working the threat at the time, and journalistic and scholarly accounts of the attacks.

Interviews included officials at the Central Intelligence Agency, the Federal Bureau of Investigation, the National Security Agency, the Department of Defense, the National Security Council, the Department of State, outside experts and other individuals who possess firsthand knowledge of the Community's performance or who can offer broader insights into the challenge of counterterrorism.

One particularly helpful report was the Senate Select Committee on Intelligence's recently completed study of the attack on the USS *Cole* and the Community's performance regarding that attack.

This staff statement is intended to provide the two committees with lines of inquiry that we believe are worth pursuing with the panelists who will appear before you today. It has four elements.

First, we review briefly several major terrorist attacks or plots against the United States at home and abroad.

Second, we note several characteristics of the terrorism challenge that became increasingly apparent in the 1990s.

Third, we identify a number of important steps taken by U.S. intelligence and other agencies to combat terrorism more effectively, steps that almost certainly saved many lives.

Fourth and finally, we describe in detail several problems or issues apparent from past attacks, noting how these hindered the overall U.S. response to terrorism.

Several of these issues transcend the Intelligence Community and involve policy issues. Others were recognized early on by the Community, but were not fully resolved.

The staff has reviewed five past terrorist attacks or attempts against the United States as part of its inquiry into September 11. They are:

The 1993 bombing of the World Trade Center that killed six people and wounded another 1,000;

The 1996 attack on the U.S. military at Khobar Towers in Saudi Arabia that killed 19 Americans and wounded 500;

The 1998 attacks on the U.S. embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania. The attacks, which occurred less than 10 minutes apart, destroyed the facilities and killed 12 Americans and over 200 Kenyans and Tanzanians; more than 4,000 were injured, many permanently blinded;

The planned attacks in 1999 and 2000 around the Millennium celebrations; and

The 2000 attack on the USS *Cole,* which killed 17 sailors and wounded 39 more. Each of those is gone into in far greater detail in our staff statement, but for purposes of the oral summary, I will not repeat those details.

The Joint Inquiry Staff review of these five incidents suggest several important characteristics of the emerging terrorist threat. Some were obvious to all at the time and others only became clear in retrospect, but all required changes in U.S. counterterrorism efforts and, more broadly, within the Intelligence Community.

The characteristics include:

The emergence of a new breed of terrorist, practicing a new form of terrorism, different from the state-sponsored, limited-casualty terrorism of the 1960s, the 1970s and the 1980s. The new terrorists were not directly sponsored by a state and sought to kill thousands or more in their attacks;

The presence of international terrorists who operated in America and were willing to conduct attacks inside America. The relative immunity from international terrorism that America had for many years enjoyed was gone. Terrorists would conduct attacks on U.S. soil and organize and raise funds in the United States for attacks overseas;

An adversary, al-Qa'ida, that is unusual in its dedication, its size, its organizational structure and its mission. Throughout the 1990s, al-Qa'ida became more skilled and attracted more adherents, making it, in essence, a small army by the end of the decade;

The existence of a sanctuary in Afghanistan that allowed al-Qa'ida to organize, to train, to proselytize, to recruit, to raise funds and to grow into a worldwide menace; and

Finally, the exploitation of permissive environments, such as Yemen, where governments were not willing or able to crack down on radical extremist activity. Unlike Afghanistan, the regimes in these countries did not necessarily support al-Qa'ida; rather, they lacked the will or the ability to stop its activities.

As these challenges emerged, the Intelligence Community and, at times, the United States Government adopted several important measures that increased America's ability to fight terrorism in general and al-Qa'ida in particular. Many of these measures can only be described obliquely or cannot be mentioned at all due to national security requirements and rightful concerns about revealing intelligence methods. Several counterterrorism efforts do, however, deserve mention.

First, the early creation of a special unit to target bin Ladin well before bin Ladin became a household name or even well known to counterterrorism specialists: The CTC created a unit dedicated to learning more about bin Ladin's activities. This unit quickly deter-

mined that bin Ladin was more than a terrorist financier, and it became the U.S. Government's focal point for expertise on and operations against bin Ladin. Later, after the 1998 embassy attacks made the threat clearer, the FBI and the NSA increased their focus on al-Qa'ida and on Islamic extremism.

Second, innovative legal strategies: In the trial of Sheikh Omar Abdul Rahman, the Department of Justice creatively resurrected the Civil War-era charge of seditious conspiracy, enabling the U.S. Government to prosecute and jail individuals planning terrorist attacks in America.

Aggressive renditions: Working with a wide array of foreign governments, the CIA helped deliver dozens of suspected terrorists to the United States or allied countries. These renditions often led to confessions and disrupted terrorist plots by shattering cells and removing key individuals.

Improved use of foreign liaison services: As al-Qa'ida emerged, several CIA officials recognized that traditional U.S. intelligence techniques were of limited value in penetrating and in countering the organization. They understood that foreign liaison could act as a tremendous force multiplier, and tried to coordinate and streamline what had been an ad hoc process.

Strategic warning on the risks to U.S. interests overseas: After the bombings of the U.S. embassies in Kenya and Tanzania in 1998, the CIA clearly and repeatedly provided warnings to senior U.S. policymakers, warnings that reached a crescendo in the summer of 2001. Policymakers from both the Clinton and the Bush administrations have testified that the Intelligence Community repeatedly warned them that al-Qa'ida was both capable of and seeking to inflict mass casualties on America.

Expansion of the FBI overseas: FBI Director Louis Freeh greatly expanded the number of legal attache offices and focused them more on countries in which terrorism was prevalent or which were important partners against terrorism.

By September 11, there were 44 legal attache offices, up from 16 in 1992. Given the increasing role the FBI and the Department of Justice were playing in counterterrorism, these offices helped ensure that domestic and overseas efforts were better coordinated.

Augmenting the Joint Terrorism Task Forces, or JTTFs: The Joint Terrorism Task Force model was originally created to improve coordination between the FBI and the New York Police Department. The first World Trade Center attack led to the expansion of the JTTFs to other cities and led to the inclusion of CIA officers in several task forces.

Improved information sharing: Intelligence officials and policymakers took several measures to improve information-sharing on terrorism among leading U.S. Government agencies. The National Security Council revived the interagency process on terrorism and threat warning, resulting in regular senior policymaker meetings concerning terrorism. The NSA and the CIA held regular video conferences among analysts after the 1998 embassy bombings. Although many weaknesses remain, the FBI and the CIA took steps to increase collaboration, which had been extremely poor in the early 1990s, and established rotations in each other's counterterrorism units.

Despite these measures to better fight terrorism, the Community response was limited by a number of factors, including interpretations of U.S. law and overall U.S. counterterrorism policy.

Among these factors were, first, continued terrorist sanctuary. Up until September 11, al-Qa'ida raised an army in Afghanistan. Despite the Intelligence Community's growing recognition that Afghanistan was churning out thousands of trained radicals, there was little effort to integrate all the instruments of national power—diplomatic, intelligence, economic and military—to address this problem.

Both the Clinton and the Bush administrations took some steps to address the problem of Afghanistan. Former National Security Adviser Berger has testified that after August, 1998, "The President authorized a series of overt and covert actions to get bin Ladin and his top lieutenants." None of these actions appear to have ultimately hindered terrorist training or al-Qa'ida's ability to operate from Afghanistan. However, Berger also testified that there was little public or congressional support for an invasion of Afghanistan before September 11.

Deputy Secretary of State Armitage and Deputy Secretary of Defense Wolfowitz have testified that by the time of the September 11 attacks, the Bush administration was far along, but not finished, with a policy review that called for more aggressive policy against the Taliban and against al-Qa'ida in Afghanistan. They were not, however, actively using the military against terrorism before this time.

In addition, al-Qa'ida exploited the laxness of other countries' counterterrorism efforts or the limits imposed by their legal systems. As the National Commission on Terrorism, the Bremer Commission, reported in 1998, "Some countries use the rhetoric of counterterrorist cooperation, but are unwilling to shoulder their responsibilities in practice, such as restricting the travel of terrorists throughout their territory."

A law enforcement approach to terrorism: In part because options such as military force were not promising or deemed feasible, the United States defaulted to countering terrorism primarily through arrests and trials. The use of the law enforcement approach had several weaknesses, including allowing al-Qa'ida continued sanctuary in Afghanistan. The reliance on law enforcement when individuals fled to a hostile country, such as Iran or the Taliban's Afghanistan, appears particularly ineffective, as the masterminds are often beyond the reach of justice.

During our interviews, one FBI agent scorned the idea of using the FBI to take the lead in countering al-Qa'ida, noting that all the FBI can do is arrest and prosecute. He noted that they cannot shut down training camps in hostile countries. In his view, "It is like telling the FBI after Pearl Harbor, 'Go to Tokyo and arrest the Emperor.'" In his opinion, a military solution was necessary because, "The Southern District doesn't have any cruise missiles."

Although the investigations contributed greatly to America's understanding of al-Qa'ida, the emphasis on prosecutions at times led to the diversion of considerable resources away from intelligence-gathering about future threats.

Limited FBI aggressiveness at home: The FBI responded unevenly at home, with only some field offices devoting significant resources to al-Qa'ida. An overall assessment of the risk to America was not prepared, and much of the FBI's counterterrorism effort was concentrated abroad. This situation reflected a huge gap in the U.S. Government's counterterrorism structure, a lack of focus on how an international terrorist group might target the United States itself.

No agency appears to have been responsible for regularly assessing the threat to the homeland. In his testimony before the Joint Committees on September 19, Deputy Secretary of Defense Wolfowitz opined that an attack against the United States had fallen between the cracks in the Intelligence Community's division of labor. He noted that, "There is a problem of where responsibility is assigned." The CIA and the NSA followed events overseas, and their employees saw their job as passing relevant threat information to the FBI. The FBI, on the other hand, did not have the strategic analytic capability independent of individual operations to prepare comprehensive assessments of U.S. vulnerability and relied heavily on the CIA for much of its analysis.

Attention to terrorist activity in the United States did, however, often increase after an attack when the links between the extremists in the United States and those overseas became better known. For example, former FBI Counterterrorism Chief Dale Watson said that he only knew of three al-Qa'ida suspects in the United States before the 1998 Africa embassy bombings, but some 200 FBI counterterrorism cases were opened after those bombings.

Lack of a coordinated Intelligence Community response: The main intelligence agencies often did not collaborate. They, at times, did not work together to target terrorists, and officers at one agency often unknowingly withheld information that was needed by another. Classification of data and legal restrictions magnified the problem. Even the CTC, the Intelligence Community's counterterrorism organization that was expressly designed to foster a Community-wide response, suffered from parochialism. Interviews at the NSA, the DIA, and the FBI indicate that many officials there saw the CTC primarily as a CIA rather than a Community organization.

Beyond the CTC, the JTTFs did not always include CIA officers. Of the 35 JTTFs active on September 11, only six had CIA officers on them.

At NSA, officials contended that the responsibility for collecting information concerning foreign radicals in the United States was the responsibility of the FBI. NSA maintained that this was true even when these individuals were communicating internationally.

As a result, NSA did not use one sensitive collection technique that would have improved its chances of successful collection. NSA adopted this strategy even though its mission included the collection and exploitation of foreign communications that have one communicant in the United States, and such coverage would have been available under a FISA. NSA does not appear to have developed a systematic plan to ensure that the FBI would routinely pursue collection in cases where NSA would not do so.

The net effect of these collaboration problems was gaps in the collection and analysis of information about individuals and groups operating both in the United States and abroad.

The actions of those responsible for the attacks on September 11 demonstrate why effective integration of both domestic and foreign collection is critical in understanding fully the operations of international terrorists. We know now that several hijackers communicated extensively abroad after arriving in the United States, and at least two entered, left, and returned to the United States. Effective tracking of their activities, which would have required coordination among the agencies, might have provided important additional information.

Difficulties in sharing law enforcement and intelligence information: The walls that had developed to separate intelligence and law enforcement often hindered efforts to investigate terrorist operations aggressively, as we saw in previous testimony about the CIA and FBI action regarding hijackers Khalid al-Mihdhar and Nawaf al-Hazmi.

In addition, misunderstandings, misperceptions and cultural differences led to other types of walls that often hindered the flow of information within the Community and between the Community and other parts of the U.S. Government.

Finally, limited changes in intelligence priorities: As certain threats, including terrorism, increased in the late 1990s, none of the lower level, Tier One national security priorities were downgraded so that resources, i.e., money and people, could be reallocated. As a result, to much of the Intelligence Community, everything was a priority. The U.S. wanted to know everything about everything all the time.

For example, NSA analysts acknowledged that they had far too many broad requirements, some 1,500 formal ones, that covered virtually every situation and every target. Within these 1,500 formal requirements, there were almost 20,000 essential elements of information that were mandated by customers.

Analysts understood the gross priorities and worked the requirements that were practicable on any given day. While counterterrorism became an increasingly important concern for senior Intelligence Community officials, collection and analytic efforts did not keep pace.

In closing, as this review suggests, the Intelligence Community made several impressive advances in fighting terrorism since the end of the Cold War, but many fundamental steps were not taken. Individual components of the Community scored impressive successes or strengthened their effort against terrorism, but important gaps remained. These included many problems outside the control or the responsibility of the Intelligence Community, such as the sanctuary terrorists enjoyed in Afghanistan and the legal limits on information-sharing between intelligence and law enforcement officials.

However, another major contributing factor was that the Community did not fully learn the lessons of past attacks. On September 11, 2001, al-Qa'ida was able to exploit the gaps in the U.S. counterterrorism structure to carry out its devastating attacks.

Mr. Chairman, that concludes my statement.

Chairman GOSS. Thank you very much, Ms. Hill. As usual, that is very comprehensive.

I would draw Members to even more comprehensive versions of it that are in your books. There is a classified version, as well, which is worth reading.

Ms. HILL. Thank you, Mr. Chairman.

Chairman GOSS. Before introducing our witnesses, the committees have received statements for the record that will not be accompanied today by oral testimony, but I should note, one of these statements was submitted by Dr. Bruce Hoffman of the RAND Corporation, who is an expert on terrorism; and the second was provided by Mr. Kie Fallis, a counterterrorism analyst formerly assigned to the Defense Intelligence Agency.

I ask unanimous consent that Dr. Hoffman's and Mr. Fallis's statements be made part of the record of this hearing.

Without objection, so ordered.

[The statement of Dr. Hoffman follows:]

JOINT INQUIRY STAFF REQUEST

Response from
Dr. Bruce Hoffman
Vice President, External Affairs and
Director, RAND Washington Office
The RAND Corporation

20 August 2002

It should be emphasized that the views and conclusions expressed herein are those of Dr. Bruce Hoffman *only* and do not represent those of any organizations or entities to which he is affiliated.

How has the threat terrorists pose to the United States changed since the end of the cold war?

Starting in the early 1990s, terrorism underwent a profound change. New adversaries, with new motivations and new rationales surfaced to challenge much of the conventional wisdom on both terrorists and terrorism. Critically, many analysts both inside and external to government were slow to recognize these changes or even worse dismissed them. Accordingly, throughout most of the 1990s our conceptions and policies remained largely the same, dating from terrorism's emergence as a global security problem more than thirty years before. These conceptions originated, and took hold, during the Cold War: when radical left-wing terrorist groups then active throughout the world were widely regarded as posing the most serious threat to Western security.[1] The irrelevance of this thinking to various aspects of the "new terrorist" problem as it

[1]Some observers argued that these groups were in fact part of a world-wide communist plot orchestrated by Moscow and implemented by its client states. See especially Claire Sterling, *The Terror Network: The Secret War of International Terrorism* (New York: Holt, Rinehart and Winston, 1981).

crystallized during the 1990s is perhaps most clearly evidenced by the changes in our notions of the "stereotypical-type terrorist organization."

Terrorist groups, for example, were once recognizable mostly as a collection of individuals belonging to an organization with a well-defined command and control apparatus, who were engaged in conspiracy as a full-time avocation, living underground while constantly planning and plotting terrorist attacks and who at times were under the direct control, or operating at the express behest of, a foreign government.[2] These groups, moreover, had a defined set of political, social or economic objectives and often issued communiqués taking credit for and explaining their actions. Accordingly, however disagreeable or repugnant the terrorists and their tactics may have been, we at least knew who they were and what they wanted.

During the past decade, however, these more "traditional" and familiar types of ethnic/nationalist-separatist and ideological organizations[3] were joined by a variety of "entities" with arguably less comprehensible nationalist or ideological motivations. This "new generation" of terrorist groups embraced not only far more amorphous religious and sometimes millenarian aims but also were less cohesive organizational entities, with a more diffuse structure and membership. In this respect, the emergence of either obscure, idiosyncratic millenarian movements[4] or zealously nationalist religious groups[5] represented a very different and potentially far more lethal threat than the more "traditional" terrorist adversaries.

For example, although the total volume of terrorist incidents world-wide declined in the 1990s, according to Department of State statistics presented in the annual *Global Patterns of International Terrorism* publications, the proportion of persons killed in terrorist incidents generally increased. Hence, while terrorists were arguably less active, they were nonetheless becoming more lethal. The reasons for terrorism's increasing lethality are complex and variegated, but can generally be attributed to the change in the

---

[2]To cite the most obvious, and perhaps best known, example: In the late 1980s, Colonel Qaddafi reputedly commissioned the Japanese Red Army (JRA) to carry out attacks against American and British targets (in retaliation for the 1986 U.S. air strike against Libya). The JRA used the name "Anti-Imperialist International Brigades" in claiming responsibility for these operations.

[3]That is, the variety of aforementioned radical leftist (e.g., Marxist-Leninist/Maoist/Stalinist movements) organizations active in years past (such as Germany's Red Army Faction and Italy's Red Brigades) as well as the such stereotypical ethnic/nationalist and separatist terrorist groups like the PLO, PIRA, Basque ETA, etc.

[4]Such as the Japanese Aum Shinrikyo religious sect who committed the March 1995 nerve gas attack on the Tokyo subway.

[5] Such as Hamas, Palestine Islamic Jihad, the Egyptian Islamic Jihad, the Egyptian Islamic Organizations, the Armed Islamic Group in Algeria and, of course, al-Qa'ida.

motivations and intentions as embodied in the growth of the number of terrorist groups motivated by a religious imperative.

The emergence of terrorism motivated by a religious imperative encapsulates the confluence of new adversaries, motivations and rationales affecting terrorist patterns today. The connection between religion and terrorism is not new.[6] However, while religion and terrorism do share a long history, until the 1990s this particular variant had largely been overshadowed by ethnic- and nationalist-separatist or ideologically motivated terrorism. Indeed, none of the 11 identifiable terrorist groups[7] active in 1968 (the year credited with marking the advent of modern, international terrorism) could be classified as "religious."[8] Not until 1980 in fact—as a result of the repercussions from the revolution in Iran the year before—do the first "modern" religious terrorist groups appear:[9] but they amount to only two of the 64 groups active that year. Twelve years later, however, the number of religious terrorist groups had increased nearly six-fold, representing a quarter (11 of 48) of the terrorist organizations who carried out attacks in 1992. Significantly, this trend not only continued, but accelerated. By 1994, a third (16) of the 49 identifiable terrorist groups could be classified as religious in character and/or motivation. In 1995, their number increased yet again, to account for nearly half (26 or 46 percent) of the 56 known terrorist groups active that year. Thus, by the middle of the decade, the rise of religious terrorism was clear.

The violent record of various Shi'a Islamic groups during the prior decade already evidenced the higher levels of lethality of religious terrorism. For example, although these organizations committed only eight percent of all recorded international terrorist incidents between 1982 and 1989, they were nonetheless responsible for nearly 30 percent of the total number of deaths during that period.[10] Indeed, some of the most significant

[6]As David C. Rapoport points out in his seminal study of what he terms "holy terror," until the nineteenth century, "religion provided the only acceptable justifications for terror" (see David C. Rapoport, "Fear and Trembling: Terrorism in Three Religious Traditions," *American Political Science Review*, Vol. 78, No. 3, September 1984, p. 659).

[7]Numbers of active, *identifiable* terrorist groups from 1968 to the present are derived from The RAND Chronology of International Terrorist Incidents.

[8]Admittedly, many contemporary terrorist groups—such as the overwhelmingly Catholic Provisional Irish Republic Army; their Protestant counterparts arrayed in various Loyalist paramilitary groups like the Ulster Freedom Fighters, the Ulster Volunteer Force, and the Red Hand Commandos; and the predominantly Muslim Palestine Liberation Organization—all have a strong religious component by dint of their membership. However, it is the political and not the religious aspect that is the dominant characteristic of these groups, as evidenced by the pre-eminence of their nationalist and/or irredentist aims.

[9]The Iranian-backed Shi'a groups *al-Dawa* and the Committee for Safeguarding the Islamic Revolution.

[10]According to The RAND Chronology of International Terrorist Incidents, between 1982 and 1989 Shi'a terrorist groups committed 247 terrorist incidents but were responsible for 1057 deaths.

terrorist acts of recent years have all had some religious element present.[11] More disturbing is that in some instances the perpetrators' aims go beyond the establishment of some theocracy amenable to their specific deity,[12] but have embraced mystical, almost transcendental, and divinely inspired imperatives.[13]

Religious terrorism[14] tends to be more lethal than secular terrorism because of the radically different value systems, mechanisms of legitimization and justification, concepts of morality, and Manichean worldviews that directly affect the "holy terrorists" motivation. For the religious terrorist, violence first and foremost is a sacramental act or divine duty: executed in direct response to some theological demand or imperative and justified by scripture. Religion, therefore functions as a legitimizing force: specifically sanctioning wide scale violence against an almost open-ended category of opponents (e.g., all peoples who are not members of the religious terrorists' religion or cult). This explains why clerical sanction is so important for religious terrorists[15] and why religious figures are often required to "bless" (e.g., approve) terrorist operations before they are executed.

---

[11]These include: the July 1994 suicide bomb truck attack on a Jewish community center in Buenos Aires, Argentina; the March 1995 nerve-gas attack on the Tokyo subway perpetrated by a Japanese cult, the Aum Shinrikyo; the series of indiscriminate bombings that rocked France between July and October 1995 and again in December 1996; the assassination in November 1995 of Prime Minister Itzhak Rabin in Israel (and its attendant significance as the purported first step in a campaign of mass murder designed to disrupt the peace process); the bombings of a joint Saudi-American military training center in Riyadh in November 1995 and of a U.S. Air Force barracks in Dhahran the following June; the attack on Western tourists in Luxor in November 1997; the bloody succession of bloody suicide bombings carried out by Hamas and Palestine Islamic Jihad since 1994; and the al-Qa'ida attacks in recent years on the two U.S. embassies in East Africa, the U.S.S. Cole in Aden harbor, and of course the September 11th attacks.

[12]For example, the creation of Islamic republics modeled on Iran in predominantly Muslim countries like Algeria, Egypt and Saudi Arabia.

[13]The Aum Shinrikyo's nerve-gas attacks on the Tokyo subway in March 1995 as part to overthrow the Japanese government and establish a new Japanese state based on the worship of the group's founder and Shokho Ashara.

[14]For a more complete and detailed discussion of this particular category of terrorist organization, see Bruce Hoffman, "Holy Terror": The Implications of Terrorism Motivated By A Religious Imperative," *Studies in Conflict and Terrorism*, vol. 18, no. 4 (Winter 1995), which was also published in the RAND Paper series, under the same title, as P-7834 in July 1993. See also the more complete discussion in Bruce Hoffman, *Inside Terrorism* (NY: Columbia Univ. Press, 1998), pp. 87-130.

[15]For example, the *fatwa* (Islamic religious edict) issued by Iranian Shi'a clerics calling for Salman Rushdie's death; the "blessing" given to the bombing of New York City's World Trade Center by the Egyptian Sunni cleric, Sheikh Omar Abdel Rahman; and the dispensation given by Jewish rabbis to right-wing Jewish extremist violence against Arabs in Israel and the West Bank and Gaza; the approval given by Islamic clerics in Lebanon for Hezbollah operations and by their counterparts in the Gaza Strip for Hamas attacks; and, the pivotal role played by Shoko Ashara, the religious leader of Japan's Aum sect, over his followers. Although bin Laden himself lacks formal theological training and credentials, he has nonetheless issues fatwas to justify al-Qa'ida attacks on American and other western targets, including against civilians.

Do Islamist radicals pose a different type of danger than do leftist or nationalist groups? How does the difference manifest itself?

The most alarming aspect of the attacks on September 11th is that they conform to a trend in international terrorism that has emerged in recent years and has been almost exclusively linked to Islamic radicals: the infliction of mass, indiscriminate casualties by enigmatic adversaries, striking far beyond terrorism's traditional operational theaters in Europe and the Middle East. By contrast, terrorism, as noted above, was formerly practiced by distinct, numerically constrained organizational entities that had a defined set of political, social or economic objectives and who also often issued communiqués taking credit for, and explaining in great detail, their actions.[16] Hence, however disagreeable or distasteful their aims and motivations may have been, these groups' ideology and intentions were at least comprehensible—albeit politically radical and personally fanatical.

Most significantly, however, these more familiar terrorist groups engaged in highly selective and mostly discriminate acts of violence that were directed against a comparatively narrow range of targets. Moreover, rarely did these groups venture outside their self-proclaimed operational area (i.e., mostly their own or neighboring countries or established international centers and global cross-roads of diplomacy and commerce) to carry out attacks. Therefore Palestinian and Lebanese terrorists frequently operated in Europe and on occasion the IRA might strike in Germany or the ETA in France. For nearly three decades, the locus of *international* terrorism accordingly remained firmly entrenched in Europe and the Middle East. Only occasionally did it spill over into Asia and Latin America and almost never into Africa and the United States, itself (the sites of the most spectacular al-Qa'ida operations).

Finally, these groups were often numerically small. According to the U.S. Department of Defense, neither the Japanese Red Army nor the Red Army Faction, for example, ever numbered more than 20 to 30 hard-core members. The Red Brigades were hardly larger, with a total of fewer than 50 to 75 dedicated terrorists. Even the IRA and ETA could only call on the violent services of perhaps some 200-400 activists whilst the feared Abu Nidal Organization was limited to some 500 men-at-arms at any given time.[17]

---

[16]Indeed, some groups—like the Provisional Irish Republican Army—not only claimed responsibility for attacks, but also issued warnings in advance of such operations.

[17]See the authoritative membership figures published in the U.S. Department of Defense, *Terrorist Group Profiles* (Washington, D.C.: U.S. Government Printing Office, 1988), pp. 5, 35, 61, 64, 56, and 118.

The September 11th attacks, like those also perpetrated by Islamic radicals on the American embassies in Kenya and Tanzania three years earlier, diverge dramatically from these established patterns. First, rather than attempting either to limit casualties, the terrorists clearly intended to inflict widespread, indiscriminate casualties among thousands of innocent people in order to achieve their objective.

Second, both sets of coordinated, near-simultaneous terrorist operations occurred in regions of the world that had remained relatively outside the maelstrom of international terrorism. For exactly this reason, masterminds of the attacks probably regarded Kenya and Tanzania and later the United States as irresistibly attractive operational environments precisely because of this past immunity. This factor alone must send disquieting reverberations to other parts of the globe who have hitherto been unaffected by international terrorism. In this respect, *no country* can any longer feel completely secure. Already, in 1992 and again 1994, Argentina—a country similarly located in a region of the globe traditionally outside the ambit of international terrorism—became tragically enmeshed in distant struggles with the massive truck-bombings of the Israeli embassy in Buenos Aires and two years later of a Jewish community center in that same city.

In recent years, bin Laden not only publicly declared war on the United States because of its support for Israel and the presence of American military forces in Saudi Arabia, but has issued *fatwas*, or Islamic religious edicts, thereby endowing his calls for violence with an incontrovertible theological as well as political justification. To this end, tens of thousands reportedly have been trained by bin Laden in Afghanistan and the Sudan over the past decade.[18]

In sum, the resurgence of terrorism motivated by a religious imperative could hardly be more palpable or different from previous waves of terrorism over the past three decades.

Is al-Qa'ida a particularly dangerous unusual adversary?

Al-Qa'ida is a particularly dangerous adversary because it is a remarkably adaptive and nimble organization. The fact that is able to function on a number of different operational levels (with varying degrees of command and control from some central authority exercised) also means that it does not have one set modus operandi nor any single identifiable footprint. This is at least partially a reflection of the organizational and

[18]Douglas Frantz and Raymond Bonner, "Web of Terrorism: Investigators See Links to bin Laden in Gaza and Across Europe," New York Times, 23 September 2001.

operational abilities, vision, attention to detail and level of planning and patience and finally business and management acumen that bin Laden has brought to the group I his role as charismatic leader.

This constellation of characteristics was clearly evident in the enormity and sheer scale of the simultaneous suicide attacks carried out by al-Qa'ida on September 11th eclipse anything we have previously seen in terrorism. Among the most significant characteristics of the operation were its ambitious scope and dimensions; impressive coordination and synchronization; and the unswerving dedication and determination of the 19 aircraft hijackers who willingly and wantonly killed themselves, the passengers and crews of the four aircraft they commandeered and the approximately three thousand persons working or visiting both the World Trade Center and the Pentagon.

Indeed, in terms of lethality alone the September 11th attacks are without precedent. For example, since 1968, the year credited with marking the advent of modern, international terrorism, one feature of international terrorism has remained constant despite variations in the number of attacks from year to year. Almost without exception,[19] the United States has annually led the list of countries whose citizens and property were most frequently attacked by terrorists.[20] But, until September 11th, over the preceding 33 years a total of no more than perhaps 1,000 Americans had been killed by terrorists either overseas or even within the U. S. itself. In less than 90 minutes that day, nearly three times that number were killed.[21] To put those uniquely tragic events in context, during the entirety of the 20th Century no more than 14 terrorist operations killed more than 100 persons at any one time.[22] Or, viewed from still another perspective, until September 11th, no terrorist single operation had ever killed more than 500 persons at one

[19] The lone exception was 1995, when a major increase in non-lethal terrorist attacks against property in Germany and Turkey by the PKK (Kurdistan Workers' Party) not only moved the US to the number two position but is also credited with accounting for that year's dramatic rise in the total number of incidents from 322 to 440. See Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 1999*. Washington, D.C., U.S. Department of State Publication 10321, April 1996, p. 1.

[20] Several factors can account for this phenomenon, in addition to America's position as the sole remaining superpower and leader of the free world. These include the geographical scope and diversity of America's overseas business interests, the number of Americans traveling or working abroad, and the many U.S. military bases around the world.

[21] See "Timetables of the Hijacked Flights," in Reporters, Writers, and Editors of Der Spiegel Magazine, *Inside 9-11: What Really Happened* (NY: St. Martin's, 2002), pp. 261-262.

[22] Brian M. Jenkins, "The Organization Men: Anatomy of a Terrorist Attack," in James F. Hoge, Jr. and Gideon Rose, *How Did This Happen? Terrorism and the New War* (NY: Public Affairs, 2001), p.5.

time.[23] Whatever the metric, therefore, the attacks that day were unparalleled in their severity and lethal ambitions.

Significantly, too, from a purely terrorist operational perspective, *spectacular* simultaneous attacks such as took place on September 11th—using far more prosaic and arguably conventional means of attack (such as car bombs, for example)—are relatively uncommon. For reasons not well understood, terrorists typically have not undertaken coordinated operations. This was doubtless less of a choice than a reflection of the logistical and other organizational hurdles and constraints that all but the most sophisticated terrorist groups are unable to overcome. Indeed, this was one reason why we were so galvanized by the synchronized attacks on the American embassies in Nairobi and Dar-es-Salaam three years ago. The orchestration of that operation, coupled with its unusually high death and casualty tolls, stood out in a way that, until September 11th, few other terrorist operations had. During the 1990s, perhaps only one other terrorist operation evidenced those same characteristics of coordination and high lethality: the series of attacks that occurred in Bombay in March 1993, when ten coordinated car bombings rocked the city, killing nearly 300 persons and wounding more than 700 others.[24] In the preceding two decades there were comparatively few successfully executed, simultaneous terrorist spectaculars.[25]

Finally, the September 11th attacks not only showed a level of patience and detailed planning rarely seen among terrorist movements today, but the hijackers stunned the world with their determination to kill themselves as well as their victims. Suicide attacks differ from other terrorist operations precisely because the perpetrator's own death is a

[23] Some 440 persons perished in a 1978 fire deliberately set by terrorists at a movie theater in Abadan, Iran.

[24] Celia W. Dugger, "Victims of '93 Bombay Terror Wary of U.S. Motives," *New York Times*, 24 September 2001.

[25] Apart from the attacks on the same morning in October 1983 of the U.S. Marine barracks in Beirut (241 persons were killed) and a nearby French paratroop headquarters (where 60 soldiers perished); the 1981 hijacking of three Venezuelan passenger jets by a mixed commando of Salvadoran leftists and Puerto Rican *independistas*; the attacks on the Rome and Vienna airports staged by the Abu Nidal Group in December 1986; and the dramatic 1970 hijacking of four commercial aircraft by the PFLP (Popular Front for the Liberation of Palestine), two of which were brought to and then dramatically blown up at Dawson's Field in Jordan, there have been comparatively few successfully executed, simultaneous terrorist spectaculars. Several other potentially high lethality simultaneous attacks during the 1980s were averted. These include, a 1985 plot by Sikh separatists in India and Canada to simultaneously bomb three aircraft while inflight (one succeeded: the downing of an Air India flight while en route from Montréal, Québec, to London, England, in which 329 persons were killed); a Palestinian plot to bomb two separate Pan Am flights in 1982 and perhaps the most infamous and ambitious of all pre-September 11th incidents: Ramzi Ahmed Yousef's "Bojinka" plan to bring down 12 American airliners over the Pacific. See Jenkins, "The Organization Men: Anatomy of a Terrorist Attack." p. 6.

requirement for the attack's success.[26] This dimension of terrorist operations, however, arguably remains poorly understood. In no aspect of the September 11th attacks is this clearer than in the debate over whether all 19 of the hijackers knew they were on a suicide mission or whether only the four persons actually flying the aircraft into their targets did. It is a debate that underscores the poverty of our understanding of bin Laden, terrorism motivated by a religious imperative, in particular, and the concept of martyrdom.

The so-called *Jihad Manual*, discovered by British police in March 2000 on the hard drive of an al-Qa'ida member's computer is explicit about operational security (OPSEC) in the section that discusses tradecraft. For reasons of operational security, it states, only the leaders of an attack should know all the details of the operation and these should only be revealed to the rest of unit at the last possible moment.[27] Schooled in this tradecraft, the 19 hijackers doubtless understood that they were on a one-way mission from the time they were dispatched to the US on their mission of martyrdom. Indeed, the video tape of bin Laden and his chief lieutenant, Dr. Ayman Zawahiri, recently broadcast by the Arabic television news station *al Jazeera* contains footage of one of the hijackers acknowledging his impending martyrdom in an allusion to the forthcoming September 11th attacks. On the tape, Ahmad Ibrahim Al Haznawi, one of the hijackers who provided the "muscle" and was not the pilot aboard the American Airlines flight which crashed into the Pentagon on September 11th, contained a date and place name beside his reproduced signature indicating that it was recorded in Khandahar, Afghanistan around March 2001. In it, Al Haznawi bluntly explains that he is a martyr being deployed to America to kill Americans.[28]

The phenomenon of terrorist martyrdom in Islam has of course long been discussed and examined. The act itself can be traced back to the Assassins, an off-shoot of the Shia Ismaili movement, who some 700 years ago waged a protracted struggle against the European Crusaders' attempted conquest of the Holy Land. The Assassins embraced an ethos of self-sacrifice, where martyrdom was regarded as a sacramental act—a highly desirable aspiration and divine duty commanded by religious text and communicated by

---

[26] See Yoram Schweitzer, "Suicide Terrorism: Development and Main Characteristics," in The International Policy Institute for Counter-Terrorism at the Interdisciplinary Center Herzliya, *Countering Suicide Terrorism: An International Conference* (Jerusalem and Hewlett, NY: Gefen, 2001), p. 76.

[27] See bin Laden's comments about this on the videotape released by the U.S. Government in November 2001, a verbatim transcript of which is reproduced in Reporters, Writers, and Editors, *Inside 9-11: What Really Happened*, pp. 313-321.

[28] See Howard Schneider and Walter Pincus, "Bin Laden Video Includes Sept. 11 Praise," *Washington Post*, 16 April, 2002.

clerical authorities. This is still evident today. An important additional motivation then as now was the promise that the martyr would feel no pain in the commission of his sacred act and would then ascend immediately to a glorious heaven, described as a place replete with "rivers of milk and wine . . . lakes of honey, and the services of 72 virgins," where the martyr will see the face of Allah and later be joined by 70 chosen relatives.[29] The last will and testament of Muhammad Atta, the ringleader of the September 11th hijackers, along with a "primer" for martyrs that he wrote, entitled, "The Sky Smiles, My Young Son," clearly evidences such beliefs.[30]

Contrary to popular belief and misconception, suicide terrorists are not exclusively derived from the ranks of the mentally unstable, economically bereft, or abject, isolated loners. In fact many of the hijackers' relatively high levels of education, socio-economic status and stable family ties were characteristics not uncommon among terrorists deployed on suicide missions.[31] In point of fact, In the more sophisticated and competent terrorist groups, such as the LTTE (Liberation Tigers of Tamil Eelam, or Tamil Tigers), it is precisely the most battle-hardened, skilled and dedicated cadre who enthusiastically volunteer to commit suicide attacks.[32]

We also failed to understand and comprehend Usama bin Laden: his vision, his capabilities, his financial resources and acumen as well as his organizational skills. For bin Laden, the weapons of modern terrorism critically are not only the traditional guns and bombs, but also the mini-cam, videotape, television and the Internet. The professionally produced and edited two hour al-Qa'ida recruitment videotape that bin Laden circulated throughout the Middle East during the summer of 2001—which according to Bergen also subtly presaged the September 11th attacks—is exactly such an example of what Peter Bergen has described as bin Laden's nimble exploitation of "twenty-first-century communications and weapons technology in the service of the most extreme, retrograde reading of holy war."[33] The tape, with its graphic footage of infidels attacking Muslims in Chechnya, Kashmir, Iraq, Israel, Lebanon, Indonesia and Egypt;

---

[29] "Wedded to death in a blaze of glory—Profile: The suicide bomber," *The Sunday Times* (London), 10 March 1996; and Christopher Walker, "Palestinian 'Was Duped into Being Suicide Bomber'," *The Times* (London), 27 March 1997.

[30] See Reporters, Writers, and Editors, *Inside 9-11*, on pp. 304-313.

[31] See, for example, Jenkins, "The Organization Men," p. 8.

[32] See in particular the work of Dr. Rohan Gunaratna of St Andrews University in this area and specifically his "Suicide Terrorism in Sri Lanka and India," in International Policy, *Countering Suicide Terrorism*, pp. 97-104.

[33] Peter L. Bergen, *Holy War, Inc.: Inside the Secret World of Osama bin Laden* (NY: Free Press, 2001), p. 27.

children starving under the yoke of United Nations economic sanctions in Iraq; and most vexatiously, the accursed presence of "Crusader" military forces in the holy land of Arabia, was subsequently converted to CD-ROM and DVD formats for ease in copying onto computers and loading onto the world-wide web for still wider, global dissemination. An even more stunning illustration of his communications acumen and clever manipulation of media was the pre-recorded, pre-produced, B-roll, or video clip, that bin Laden had queued and ready for broadcast within hours of the commencement of the American air strikes on Afghanistan on Sunday, October 7th.

In addition to his adroit marrying of technology to religion and of harnessing the munificence of modernity and the West as a weapon to be wielded against his enemies, bin Laden has demonstrated uncommon patience, planning and attention to detail. According to testimony presented at the trial of three of the 1998 East African embassy bombers in Federal District Court in New York last year by a former bin Laden lieutenant, Ali Muhammad, [34] planning for the attack on the Nairobi facility commenced nearly five years before the operation was executed. Muhammad also testified that bin Laden himself studied a surveillance photograph of the embassy compound, pointing to the spot in front of the building where he said the truck bomb should be positioned. Attention has already been drawn to al-Qa'ida's ability to commence planning of another operation before the latest one has been executed in the case of the embassy bombings and the attack 27 months later on the *U.S.S. Cole*. Clearly, when necessary, bin Laden devotes specific attention—perhaps even to the extent of micro managing—various key aspects of al-Qa'ida "spectaculars." In the famous videotape discovered in an al-Qa'ida safe house in Afghanistan that was released by the U.S. government in December 2001, bin Laden is seen discussing various, intimate details of the September 11th attack. At one point, bin Laden explains how "we calculated in advance the number of casualties from the enemy, who would be killed based on the position of the tower. We calculated that the floors [that] would be hit would [be] three or four floors. I was the most optimistic of them all. . . . due to my experience in this field . . . ." alluding to his knowledge of construction techniques gleaned from his time with the family business. [35] Bin Laden also knew that Muhammad Atta was the operation's leader[36] and states that he

[34] Ali Muhammad, a former major in the Egyptian Army, enlisted in the U.S. Army, where he served as a non-commissioned officer at Fort Bragg, North Carolina, teaching U.S. Special Forces about Middle Eastern culture and politics. Mohammed, among other al-Qa'ida operatives, like Wadi el-Hoge, demonstrates how al-Qa'ida found the U.S. a comfortable and unthreatening operational environment. See Hoffman, "Terrorism's CEO," www.theatlantic.com/unbound/interviews/int2002-01-09.html.

[35] Reporters, Writers, and Editors, *Inside 9-11*, p. 317.

and his closest lieutenants "had notification [of the attack] since the previous Thursday that the event would take place that day [on September 11th]."[37]

The portrait of bin Laden that thus emerges is richer, more complex, and more accurate than the simple caricature of a hate-filled, mindless fanatic. "All men dream: but not equally," T.E. Lawrence, the legendary Lawrence of Arabia, wrote. "Those who dream by night in the dusty recesses of their minds wake in the day to find that it was vanity: but the dreamers of the day are dangerous men, for they may act their dream with open eyes, to make it possible."[38] Bin Laden is indeed one of the dangerous men that Lawrence described. At a time when the forces of globalization, coupled with economic determinism, seemed to have submerged the role the individual charismatic leader of men beneath far more powerful, impersonal forces, bin Laden has cleverly cast himself as a David against the American Goliath: one man standing up to the world's sole remaining superpower and able to challenge its might and directly threaten its citizens.

Indeed, in an age arguably devoid of ideological leadership, when these impersonal forces are thought to have erased the ability of a single man to affect the course of history, bin Laden—despite all our efforts—managed to taunt us and strike at us for years even before September 11th. His effective melding of the strands of religious fervor, Muslim piety and a profound sense of grievance into a powerful ideological force stands—however invidious and repugnant—as a towering accomplishment. In his own inimitable way, bin Laden cast this struggle as precisely the "clash of civilizations" that America and its coalition partners have labored so hard to negate. "This is a matter of religion and creed; it is not what Bush and Blair maintain, that it is a war against terrorism," he declared in a videotaped speech broadcast over al Jazeera television on November 3, 2001. "There is no way to forget the hostility between us and the infidels. It is ideological, so Muslims have to ally themselves with Muslims."[39]

Bin Laden, though, is perhaps best viewed as a "terrorist CEO": essentially having applied business administration and modern management techniques leaned both at university and in the family's construction business[40] to the running of a transnational

---

[36] Ibid., p. 319.

[37] Ibid., p. 317.

[38] T.E. Lawrence, *Seven Pillars of Wisdom* (Harmondsworth: Penguin Books, 1977), p. 23.

[39] Neil MacFarquhar with Jim Rutenberg, "Bin Laden, in a Taped Speech, Says Attacks in Afghanistan Are a War Against Islam," *New York Times*, November 4, 2001, p. B2.

[40] Bin Laden is a graduate of Saudi Arabia's prestigious King Abdul-Aziz University, where in 1981 he obtained a degree in economics and public administration. He subsequently cut his teeth in the family business, later applying the corporate management techniques learned both in the classroom and on

terrorist organization. Indeed, what bin Laden apparently has done is to implement for al-Qa'ida the same type of effective organizational framework or management approach adapted by corporate executives throughout much of the industrialized world. Just as large, multinational business conglomerates moved during the 1990s to flatter, more linear, and networked structures, bin Laden did the same with al-Qa'ida.

Additionally, he defined a flexible strategy for the group that functions at multiple levels, using both top down and bottom up approaches. On the one hand, bin Laden has functioned like the president or CEO of a large multinational corporation: defining specific goals and aims, issuing orders, and ensuring their implementation. This mostly applies to the al-Qa'ida "spectaculars": those high-visibility, usually high-value and high-casualty operations like September 11th, the attack on the *Cole*, and the East Africa embassy bombings. While on the other hand, he has operated as a venture capitalist: soliciting ideas from below, encouraging creative approaches and "out of the box" thinking and providing funding to those proposals he finds promising. Al-Qa'ida, unlike many other terrorist organizations, therefore, deliberately has no single, set modus operandi: making it all the more formidable. Instead, bin Laden encourages his followers to mix and match approaches: employing different tactics and different means of attack and operational styles as needed. At least four different levels of al-Qa'ida operational styles can be identified:

(A) *The professional cadre.* This is the most dedicated, committed and professional element of al-Qa'ida: the persons entrusted with only the most important and high value attacks—in other words, the "spectaculars." These are the terrorist teams that are pre-determined and carefully selected, are provided with very specific targeting instructions and who are generously funded (e.g., to the extent that during the days preceding the September 11th attacks, Atta and his confederates were sending money back to their paymasters in the United Arab Emirates and elsewhere).

(B) *The trained amateurs.* These are individuals much like Ahmed Ressam, who was arrested in December 1999 at Port Angeles, Washington State, shortly after he had entered the U.S. from Canada. Ressam, for example, had some prior background in terrorism, having belonged to Algeria's Armed Islamic

---

the job to transform al Qa'ida into the world's preeminent terrorist organization. See Bergen, *Holy War, Inc.*, pp. 14-15.

Group (GIA). After being recruited into al-Qa'ida, he was provided with a modicum of basic terrorist training in Afghanistan. In contrast to the professional cadre above, however, Ressam was given open-ended targeting instructions before being dispatched to North America. He was only told was to attack some target in the U.S. that involved commercial aviation. Ressam confessed that he chose Los Angeles International Airport because at one time he had passed through there and was at least vaguely familiar with it. Also, unlike the well-funded professionals, Ressam was given only $12,000 in "seed money" and instructed to raise the rest of his operational funds from petty thievery—e.g., swiping cell phones and lap tops around his adopted home of Montreal. He was also told to recruit members for his terrorist cell from among the expatriate Muslim communities in Canada and the U.S. In sum, a distinctly more amateurish level of al-Qa'ida operations than the professional cadre deployed on September 11th; and which also relied on someone far less steeled, determined and dedicated than the hijackers proved themselves to be. Ressam, of course, panicked when he was confronted by a Border Patrol agent immediately upon entering the U.S. By comparison, nine of the 19 hijackers were stopped and subjected to greater scrutiny and screening by airport personnel on September 11th. Unlike Ressam, they stuck to their cover stories, didn't lose their nerve and, despite having aroused suspicion, were still allowed to board. Richard Reid, the individual who attempted to blow up an American Airlines passenger plane en route from Paris to Miami with an explosive device concealed in his shoe, is another example of the trained amateur. It should be emphasized, however, that as inept or even moronic as these individuals might appear, their ability to be lucky even once and then to inflict incalculable pain and destruction should not be lightly dismissed. As distinctly second-tier al-Qa'ida operatives, their masters likely see them as expendable: having neither the investment in training nor the requisite personal skills that the less numerous, but more professional, first-team al-Qa'ida cadre have.

(C) *The local walk-ins.* These are local groups of Islamic radicals who come up with a terrorist attack idea on their own and then attempt to obtain funding from al-Qa'ida for it. This operational level plays to bin Laden's self-conception as a venture capitalist. An example of the local walk-in is the group of Islamic radicals in Jordan who, observing that American and Israeli tourists often stayed at the Radisson Hotel in Amman, proposed to, and were

funded by al-Qa'ida, to attack the tourists on the eve of the millennium. Similarly, the cell of Islamic militants who were arrested in Milan in October 2001 after wiretaps placed by Italian authorities revealed discussions of attacks on American interests being planned in the expectation that al-Qa'ida might fund them, is another. A more disquieting example, however, is the group of Islamic radicals associated with, but not formally a part of, al-Qa'ida, who plotted to attack the American and Israeli embassies and the British and Australian High Commissions in Singapore, as well as a subway stop used by U.S. sailors disembarking their ships on shore leave in that city. Borrowing a page from the al-Qa'ida playbook, the Singapore plotters spent at least four years planning their attacks, conducting the same detailed and meticulous reconnaissance emblematic of other al-Qa'ida spectaculars.

(D) *Like-minded insurgent, guerrillas and terrorists.* This level embraces existing insurgent or terrorist groups who over the years have benefited from bin Laden's largesse and/or spiritual guidance; received training in Afghanistan from al-Qa'ida; or have been provided with arms, materiel and other assistance by organization. These activities reflect bin Laden's "revolutionary philanthropy": that is, the aid he provides to Islamic groups as part of furthering the cause of global jihad. Among the recipients of this assistance have been insurgent forces in Uzbekistan and Indonesia, Chechnya, the Philippines, Bosnia and Kashmir, etc. This philanthropy is meant not only hopefully to create a jihad "critical mass" out of these geographically scattered, disparate movements, but also to facilitate a quid pro quo situation, where al-Qa'ida operatives can call on the logistical services and manpower resources provided locally by these groups.

Underpinning these operational levels is bin Laden's vision, self-perpetuating mythology and skilled acumen at effective communications. His message is simple. According to bin Laden's propaganda, the U.S. is a hegemonic, status quo power; opposing change and propping up corrupt and reprobate regimes that would not exist but for American backing. Bin Laden also believes that the U.S. is risk and casualty averse and therefore cannot bear the pain or suffer the losses inflicted by terrorist attack. In this respect, bin Laden has often argued that terrorism works—especially against America. He cites the withdrawal of the U.S. Marines, following the 1983 barracks bombing, from the multi-national force deployed to Beirut and how the deaths of 18 U.S. Army Rangers

(an account of which is described in the best-selling book by Mark Bowden, *Black Hawk Down*, and current film of the same title)—a far smaller number than in Beirut a decade before—prompted the precipitous U.S. withdrawal from Somalia a decade later.

Finally, it should never be forgotten that some 20 years ago bin Laden consciously sought to make his own mark in life as a patron of *jihad*—holy war. In the early 1980s, he was drawn to Afghanistan, where he helped to rally—and even more critically, fund—the Muslim guerrilla forces resisting that country's Soviet invaders. Their success in repelling one of the world's two superpowers had a lasting impact on bin Laden. To his mind, Russia's defeat in Afghanistan set in motion the chain of events that resulted in the collapse of the USSR and the demise of communism. It is this same self-confidence coupled with an abiding sense of divinely ordained historical inevitability that has convinced bin Laden that he and his fighters cannot but triumph in the struggle against America. Indeed, he has often described the U.S. as a "paper tiger": on the verge of financial ruin and total collapse—with the force of Islam poised to push America over the precipice.

Remarkably given his mindset, bin Laden would likely cling to the same presumptions despite the destruction of the Taleban and liberation of Afghanistan during this first phase of the war against terrorism. To him and his followers, the U.S. is doing even more now than before to promote global stability (in their view: preserve the status quo) and ensure the longevity of precisely those allegedly morally bankrupt regimes in places like Egypt, Saudi Arabia, the Gulf, Pakistan, Uzbekistan and elsewhere whom bin Laden and his followers despise. In bin Laden's perception of the war in Afghanistan, most of the fighting was done by the Northern Alliance—the equivalent of the native levies of imperial times; though instead of being led by British officers as in the past, who were now guided by U.S. military special operations personnel. Moreover, for bin Laden—like guerrillas and terrorists everywhere—not losing is winning. To his mind, even if terrorism didn't vanquish his hated enemy on September 11th, he can still claim to have been responsible for having a seismic effect on the U.S., if not the entire world. Whatever else, bin Laden is one of few persons who can argue that they have changed the course of history. The U.S., in his view, itself remains fundamentally corrupt and weak, on the verge of collapse, as bin Laden crowed in the videotape released last year about the "trillions of dollars" of economic losses caused by the September 11th attacks. More recently, Ahmed Omar Sheikh, the chief suspect in the killing of the American journalist, Daniel Pearl, echoed this same point. While being led out of a Pakistani court in March,

he exhorted anyone listening to "sell your dollars, because America will be finished soon."[41]

Today, added to this fundamental enmity is now the even more potent and powerful motivation of revenge for the destruction of the Taleban and America's alleged "war on Islam." Despite overwhelming evidence to the contrary, bin Laden and his followers probably still regard the U.S. as a "paper tiger," a favorite phrase of bin Laden's, whose collapse can be attained provided al-Qa'ida survives the current onslaught in Afghanistan and elsewhere in some form or another. Indeed, although weakened, al-Qa'ida has not been destroyed and at least some of its capability to inflict pain, albeit at a greatly diminished level from September 11th, likely still remains intact. In this respect, the multi-year time lag of all prior al-Qa'ida spectaculars is fundamentally disquieting since it suggests that some new monumental operation might have already been set in motion just prior to September 11th.

In hindsight, what mistakes did the United States make with regard to the threat of terrorism? Was the U.S. government too focused on the threat of terrorists using weapons of mass destruction?

Most importantly, we were (in this case: non-government terrorism analysts) perhaps lulled into believing that mass, simultaneous attacks in general and those of such devastating potential as we saw in New York and Washington on September 11th were beyond the capabilities of most terrorists—including those directly connected to, or associated with, Usama bin Laden. The tragic events of that September day demonstrate how profoundly misplaced such assumptions were. In this respect, we perhaps overestimated the significance of our past successes (e.g., in largely foiling a series of planned terrorist operations against American targets between the August 1998 embassy bombings to the November 2000 attack on the *U.S.S. Cole*, including more than 60 instances when credible evidence of impending attack forced the temporary closure of American embassies and consulates around the world) and the terrorists' own incompetence and propensity for mistakes (e.g., Ahmad Ressam's bungled attempt to enter the United States from Canada in December 1999). Both impressive and disturbing is the likelihood that there was considerable overlap in the planning for these attacks and the one in November 2000 against the U.S.S. *Cole* in Aden: thus suggesting al-Qa'ida's

[41] Raymond Bonner, "Suspect in Killing of Reporter Is Brash and Threatening in a Pakistani Court," *New York Times*, 13 March 2002.

operational and organizational capability to coordinate major, multiple attacks at one time.[42]

Attention was also arguably focused too exclusively either on the low-end threat posed by car and truck bombs against buildings or the more exotic high-end threats, against entire societies, involving biological or chemical weapons or cyber-attacks. The implicit assumptions of much of American planning scenarios on mass casualty attacks were that they would involve germ or chemical agents or result from widespread electronic attacks on critical infrastructure. It was therefore presumed that any conventional or less extensive incident could be addressed simply by planning for the most catastrophic threat. This left a painfully vulnerable gap in our anti-terrorism defenses where a traditional and long-proven tactic—like airline hijacking—was neglected in favor of other, less conventional threats and where the consequences of using an aircraft as a suicide weapon seem to have been ignored. In retrospect, it was not the 1995 sarin nerve gas attack on the Tokyo subway and the nine attempts to use bio-weapons by Aum that should have been the dominant influence on our counterterrorist thinking, but a 1986 hijacking of a Pan Am flight in Karachi, where the terrorists' intention was reported to have been to crash it into the center of Tel Aviv and the 1994 hijacking in Algiers of an Air France passenger plane by Armed Islamic Group (GIA) terrorists, who similarly planned to crash the fuel-laden aircraft with its passengers into the heart of Paris. The lesson, accordingly, is not that we need to be unrealistically omniscient, but rather that we need to be able to respond across a broad technological spectrum of potential adversarial attacks.

We also had long consoled ourselves—and had only recently began to question and debate the notion—that terrorists were more interested in publicity than killing and therefore had neither the need nor the interest in annihilating large numbers of people. For decades, there was widespread acceptance of the observation made famous by Brian Jenkins in 1975 that, "Terrorists want a lot of people watching and a lot of people listening and not a lot of people dead."[43] While entirely germane to the forms of terrorism that existed in prior decades, for too long we adhered to this antiquated notion.

---

[42] It is now believed that planning for the attack on an American warship in Aden harbor commenced some two to three weeks before the August 1998 attacks on the East African embassies. Discussion with U.S. Naval Intelligence Service agent investigating the *Cole* attack. December 2001.

[43] Brian Michael Jenkins, "International Terrorism: A New Mode of Conflict" in David Carlton and Carlo Schaerf (eds.), *International Terrorism and World Security* (London: Croom Helm, 1975), p. 15.

On September 11th, bin Laden wiped the slate clean of the conventional wisdom on terrorists and terrorism and, by doing so, ushered in a new era of conflict.

Finally, before September 11th the United States arguably lacked the political will to sustain a long and determined counterterrorism campaign. The record of inchoate, unsustained previous efforts effectively retarded significant progress against this menace. The carnage and shock of the September 11th attacks laid bare America's vulnerability and too belatedly resulted in a sea change in national attitudes and accompanying political will to combat terrorism systematically, globally and, most importantly, without respite.[44]

How might the United States anticipate, and counter, innovative delivery means and methods that make prediction and disruption more difficult?

See the discussion immediately below.

What steps should the U.S. government take to improve the analysis of terrorist groups? What skills and methods should be emphasized?

Rather than asking what could or could not happen—which is the reflexive way we tend look at and analyze terrorist threats, we might more profitably focus on understanding what hasn't happened, and asking why these types of attacks haven't occurred and then to walk them backwards to understand the capabilities and logistics required for undertaking these operations, for the illumination this line of inquiry can shed on possible future al-Qa'ida attacks. It would also be beneficial to examine and analyze the type of terrorist incidents or attacks that have only occurred once or twice before similarly for the insight his would provide into potential future terrorist operations. These types of approaches actually remain among the most understudied and in turn conspicuous lacunae of terrorism studies. Many academic terrorism analyses when they venture into the realm of future possibilities, if at all, do so only tepidly. In the main, they are self-limited to mostly lurid hypotheses of worst case scenarios, almost exclusively involving CBRN (chemical, biological, radiological or nuclear) weapons, as opposed to trying to understand why—with the exception of September 11th—terrorists have only rarely realized their true killing potential.

Among the key unanswered questions include:

---

[44] See, for example, the discussion of two former members of the U.S. National Security Staff, Daniel Benjamin and Steven Simon, on the effects of the al-Shifa on the Clinton Administration and its counterterrorism policy post the August 1998 embassy bombings. Daniel Benjamin and Steven Simon, "A Failure of Intelligence?" in Robert B. Silvers and Barbara Epstein (eds.), *Striking Terror: America's New War* (NY: New York Review of Books, 2002), pp. 279-299.

- Why haven't terrorists regularly used man-portable surface-to-air missiles (SAMs/MANPADS) to attack civil aviation?
- Why haven't terrorists employed such simpler and more easily obtainable weapons like rocket-propelled grenades (RPGs) to attack civil aviation by targeting planes while taking off or landing?
- Why haven't terrorists used unmanned drones or one-person ultra-light or micro-light aircraft to attack heavily defended targets from the air that are too difficult to gain access to on the ground?
- Why haven't terrorists used remote-controlled (even home-made) mortars from fixed positions against targets difficult to attack or access from the ground?
- Why haven't terrorists engaged in mass simultaneous attacks with very basic conventional weapons, such as car bombs, more often?
- Why haven't terrorists used tactics of massive disruption—both mass transit and electronic (cyber)—more often?
- Why haven't terrorists perpetrated more maritime attacks, especially against cruise ships loaded with holidaymakers or cargo vessels carrying hazardous materials (such as liquefied natural gas or LNG)?
- Why haven't terrorists engaged in agricultural or livestock terrorism (which is far easier and more effective than against humans) using biological agents?
- Why haven't terrorists exploited the immense psychological potential of limited, discrete use of CBRN weapons and cyber attacks more often?
- Why haven't terrorists targeted industrial or chemical plants with conventional explosives in hopes of replicating a Bhopol with thousands dead or permanently injured?
- And, finally, why—with the exception of September 11th—do terrorists generally seem to lack the rich imaginations of Hollywood movie producers, thriller writers, and others?

Alarmingly, many of the above tactics and weapons have in fact already been used, albeit infrequently, by terrorists—and often with considerable success. The 1998 downing of a civilian Lion Air flight from Jaffna to Colombo by Tamil Tigers using a Russian-manufactured SA-14 is a case in point. The aforementioned series of nearly a dozen car bombings that convulsed Bombay in March 1993 is another. The IRA's effective paralyzing of road and rail commuting traffic around London in 1997 and 1998 is one

more as were the similar tactics used by the Japanese Middle Core to shut down commuting in Tokyo a decade earlier. And in 1997, the Tamil Tigers launched one of the few documented cyber-terrorist attacks when they shut down the servers and e-mail capabilities of the Sri Lanka embassies in Seoul, Washington, D.C., and Ottawa. The Tigers also have a special maritime suicide terrorist unit, the "Sea Tigers," that have attacked Sri Lankan naval (and on rare occasion, civilian) vessels for the more than a decade. As these examples illustrate, terrorists retain an enormous capability to inflict pain and suffering without resorting to mass destruction or mass casualties on the order of the September 11th attacks. This middle range, between worse case scenario and more likely means of attack is where the U.S. remains dangerously vulnerable. Terrorists seek constantly to identify vulnerabilities and exploit gaps in our defenses. It was precisely the identification of this vulnerability in the middle range of our pain threshold that led to the events of that tragic day.

Are there lessons the United States can learn from other countries that are appropriate for the struggle against terrorism?

A survey of the counter-terrorism lessons learned from five countries' experiences covering five key functional areas, was conducted by RAND[45] this past winter and led to four principal conclusions that are summarized below.[46]

1. Focus efforts at mid-level leaders in terrorist groups. Our analysis indicates that mid-level leaders are often more important than top decision-makers to the long-term survival of a terrorist organization. Policies aimed at removing these mid-level leaders more effectively disrupt control, communications, and operations up and down the chain of command. In addition, such policies may also inhibit a group's long-term growth by eliminating the development of future leaders. For example, Israel has often targeted the top leadership of Hezbollah and Hamas. But this policy has not resulted in a dramatic decrease in terrorist attacks or the dissolution of either group. The mid-level leaders of Hezbollah, in particular, have been able to step into the new role of top decision-makers

[45] See Bruce Hoffman and Kim Cragin, "Four Lessons from Five Countries" in *RAND REVIEW—Hitting Home: What We've Learned Since 9/11 and What We Should Do About It*, vol. 26, no. 2 (Summer 2002), pp. 42-43

[46] The five countries include Israel, the Philippines, Colombia, Peru, and the U.K. The five functional areas that we addressed are intelligence, disinformation, emergency legislation, targeting terrorist leaders and disrupting support networks.

relatively easily. In the case of Hamas, Israel managed to deport almost its entire top-level leadership in 1992. But the removal of Hamas' top (relatively more moderate) leaders served to radicalize the group – the mid-level leaders that stepped up in 1992 increased the use of suicide bombers to the extent that is seen in attacks against Israel today. These examples illustrate our conclusion that targeting the top leaders of a terrorist group is often a less effective policy. The success or failure of a terrorist organization's operations and even perhaps its longevity often depends on the ability of the mid-level leaders to step into decision-making roles or carry out operational objectives more than on the top leaders themselves.

2. *De-legitimize – do not just arrest or kill – the top leaders of terrorist groups.* The top leaders of terrorist organizations are more than just policy-makers for the group. They occupy an enormously influential and important symbolic position at the head of a terrorist organization that is often inextricably connected to that organization's very existence. Therefore the public diplomacy campaign to discredit these leaders is as, or even more, important than their actual arrest or death. Some analysts credit the arrest in 1991 of Sendero Lumioso leader Abimel Guzman for the fall of SL. But another, often overlooked, component of Fujimori's strategy was to discredit Guzman thoroughly before SL members and their support network. Fujimori did this by turning Guzman's own words against him, deliberately orchestrating public speeches in which Guzman first called for SL members to give up their weapons and then abruptly reversed himself, telling them instead to continue to fight against the government. These discrepancies essentially discredited Guzman, and SL lost all forward momentum. Turkey achieved the same success after Abdullah Ocalan, the founder and leader of the Kurdish group, the PKK, was imprisoned.

3. *Focus on disrupting support networks and trafficking activities.* A further measure involves targeting essential support and logistics networks. This tactic primarily entails focusing on the middlemen that help terrorist organizations access funds and purchase supplies in the black market: financiers and smugglers. Attention is often focused on front organizations and individuals that provide money to terrorist organizations. Our analysis, however, indicates that it would be more advantageous to expand this approach and target specifically the middlemen that (e.g.) purchase diamonds from terrorists on the black market, or individuals that (e.g.) sell weapons to terrorist organizations. This tactic is a more effective way of disrupting the everyday activities that a terrorist organization must engage in to maintain its operational capabilities. It

hinders the ability of a group to gather resources and plan sophisticated attacks in advance because they cannot rely on a steady stream of money or other essential resources. [47] For example, Colombian efforts to disrupt arms trafficking activities have been more successful than coca eradication. The Colombian military has managed to do this by focusing intelligence and investigative resources on financiers and arms trafficking middlemen (external to the FARC itself). FARC communiqués and reported discussions have indicated that the organizational leadership has become increasingly concerned about the loss of necessary weapons into the country. It may be that the Colombian Armed Forces will be able to deprive FARC of crucial supplies to the extent that such activities will impinge on the group's ability to expand or even maintain control over territory in Colombia and therefore conduct operations in the medium to long term.

4. *Establish a dedicated counter-intelligence center specifically to engage terrorist reconnaissance.* More sophisticated terrorist groups do not attack people or places without a basic level of planning and reconnaissance. Therefore arguably the greatest return on investment is in the identification and disruption of pre-attack planning as well as logistical operations. A key means of achieving this is through the discernment of the terrorists' own intelligence-gathering processes. Yet we determined that none of the countries surveyed had a dedicated, stand alone, terrorist counter-intelligence unit.[48] This misses an important opportunity for pre-empting a terrorist attack. Given the highly fluid and transnational nature of the threat that the United States is facing, we recommended that the U.S. establish a separate counter-terrorism unit dedicated specifically to identifying and targeting the intelligence gathering and reconnaissance activities of terrorist organizations.

How might the threat from al-Qa'ida and associated groups change in the future?

The more sophisticated terrorist entity is perhaps best viewed as the archetypal shark in the water. It must constantly move forward to survive and indeed to succeed. While survival entails obviating the governmental countermeasures designed to unearth and destroy the terrorists and their organizations; success is dependent on overcoming the defenses and physical security barriers designed to thwart attack. In these respects, the necessity for change in order to stay one step ahead of the counterterrorism curve compels

[47] This policy will not, however, have as dramatic an impact on groups that rely on less-sophisticated tactics in regions where it is easy to find explosives for rough devices.

[48] In contrast to the specially dedicated counter-intelligence or counter-espionage units generally found in the intelligence and security services and many law enforcement agencies throughout the world.

terrorists to change: adjusting and adapting their tactics, modus operandi, and sometimes even their weapons systems as needed.[49] The better, more determined and more sophisticated terrorists will therefore always find a way to carry on their struggle.

The loss of physical sanctuaries—the most long-standing effect that the U.S.-led war on terrorism is likely to achieve—will signal only the death knell of terrorism as we have known it. In a new era of terrorism, "virtual" attacks from "virtual sanctuaries," involving anonymous cyber assaults may become more appealing for a new generation of terrorists unable to absorb the means and methods of conventional assault techniques as they once did in capacious training camps. Indeed, the attraction for such attacks will likely grow as American society itself becomes ever more dependent on electronic means of commerce and communication. One lesson from last October's anthrax cases and the immense disruption it caused the U.S. Postal Service may be to impel more rapidly than might otherwise have been the case the use of electronic banking and other on-line commercial activities. The attraction therefore for a terrorist group to bring down a system that is likely to become increasingly dependent on electronic means of communication and commerce cannot be dismissed. Indeed, Zawahiri once scolded his followers for not paying greater attention to the fears and phobias of their enemy, in that instance, Americans' intense preoccupation with the threat of bioterrorism. The next great challenge from terrorism may therefore be in cyber space.

Similarly, the attraction to employ more exotic, however, crude weapons like low-level biological and chemical agents may also increase. Although these materials might be far removed from the heinous capabilities of true WMD (weapons of mass destruction), another lesson from last October's anthrax exposure incidents was that terrorists don't have to kill 3,000 people to create panic and foment fear and insecurity: five persons dying in mysterious circumstances is quite effective at unnerving an entire nation. Accordingly, the issue may not be as much ruthless terrorist use of some mass destruction weapon to attempt to destroy an entire city and affect its entire population as the discrete, calculated terrorist use of some chemical, biological or radiological device to achieve far-reaching psychological effects or a specific reaction from the U.S.

Concluding Observations

In thinking about future threats, we need to keep at least five imperatives in mind.

[49] Bruce Hoffman, *Inside Terrorism* (NY: Columbia Univ. Press, 1998), pp. 180-183.

First, we should recognize that terrorism is, always has been, and always will be instrumental: planned, purposeful and premeditated. The challenge that analysts face is in identifying and understanding the rationale and "inner logic"[50] that motivates terrorists and animates terrorism. It is easier to dismiss terrorists as irrational homicidal maniacs than to comprehend the depth of their frustration, the core of their aims and motivations, and to appreciate how these considerations affect their choice of tactics and targets. To effectively fight terrorism, we must gain a better understanding of terrorists and terrorism than has been the case in the past.

Second, we need to recognize that terrorism is fundamentally a form of psychological warfare. Terrorism is designed, as it has always been, to have profound psychological repercussions on a target audience. Fear and intimidation are precisely the terrorists' timeless stock-in-trade. Significantly, terrorism is also designed to undermine confidence in government and leadership and to rent the fabric of trust that bonds society. It is used to create unbridled fear, dark insecurity, and reverberating panic. Terrorists seek to elicit an irrational, emotional response. Our countermeasures therefore must be at once designed to blunt that threat but also to utilize the full range of means we can bring to bear in countering terrorism: psychological as well as physical; diplomatic as well as military; economic as well as moral.

Third, the U.S. and all democratic countries that value personal freedom and fundamental civil liberties will remain vulnerable to terrorism. The fundamental asymmetry of our inability to protect all targets all the time against all possible attacks ensures that terrorism will continue to remain attractive to our enemies. In this respect, both political leaders and the public must have realistic expectations of what can and cannot be achieved in the war on terrorism and, indeed, the vulnerabilities that exist inherently in any open and democratic society.

Fourth, the enmity felt in many places throughout the world towards the U.S. will likely not diminish. America is invariably targeted as a hegemonic, status quo power and more so as the world's lone superpower. Diplomatic efforts, particularly involving renewed public diplomacy activities are therefore needed at least to effect and influence successor generations of would-be terrorists, even if we have already missed the current generation.

Finally, terrorism is a perennial, ceaseless struggle. While a war against terrorism may be needed to sustain the political and popular will that has often been missing in the

[50] My colleague at St Andrews University, Dr Magnus Ranstorp's, formulation.

past, war by definition implies finality. The struggle against terrorism, however, is never-ending. Terrorism has existed for 2,000 years and owes its survival to an ability to adapt and adjust to challenges and countermeasures and to continue to identify and exploit its opponent's vulnerabilities. For us to succeed against terrorism, our efforts must be as tireless, innovative and dynamic as our opponents.

A Review of Four Cases

Observation	WTC I	Khobar	Millennium Plot (State piece re: culpability)	*USS Cole*
Sanctuary for key planners, linked with local idiots who are caught	XX	XX	XX	XX
Network involved many countries, often in obscure/friendly countries	XX	XX	XX	XX
Information dissemination problems	XX	?	(No)	(No)
Legal response to attack	XX	(legal and limited dip/econ pressure)	XX	(legal and disruption campaign)
International threat in the U.S. homeland	XX		XX	
Community response re: Lessons Learned				
Mass casualties as an objective	XX		XX	

Chairman GOSS. Members may submit questions for the record to follow up on matters appropriately addressed to Dr. Hoffman and Mr. Fallis.

I also ask unanimous consent that the declassified findings and recommendations from the Senate Select Committee on Intelligence inquiry into intelligence collection, reporting, analysis and warning relevant to the bombing of the USS *Cole* be placed in the record.

Without objection, so ordered.

[The information referred to follows:]

UNITED STATES SENATE
SELECT COMMITTEE ON INTELLIGENCE

INQUIRY INTO INTELLIGENCE COLLECTION, REPORTING, ANALYSIS AND WARNING RELEVANT TO THE BOMBING OF THE USS COLE

FINDINGS AND RECOMMENDATIONS

Finding #1: The Central Intelligence Agency and the National Security Agency aggressively collected and promptly disseminated raw intelligence pertaining to potential terrorist threats.

Finding #2: Although Intelligence Community analysts in Washington, D.C. often had access to intelligence available on global terrorist activities, they did not always enhance their products with historical information. As a result, field operators and analysts, with limited resources to apply to historic research, were often left with that task. The process was further hampered by limitations on intelligence-sharing. While the Intelligence Community has changed significantly its terrorism procedures, it has yet to adequately address the principal shortcomings identified in this report – lack of historical context for terrorist threat products and failure to abide by warning guidelines.

Finding #3: Intelligence available prior to the attack on the USS Cole was not provided to consumers in a formal warning product prepared and issued by the Interagency Intelligence Committee on Terrorism. Intelligence Community analysts and managers attributed the decision not to issue a warning product to both the lack of specificity in timing and target and concerns about warning fatigue. The degree of specificity required by the analysts and managers in this case was overly stringent and exceeded the existing published guidelines for an Intelligence Community Terrorist Threat Advisory.

Recommendation #1: To the Director of Central Intelligence — Not later than 90 days after the receipt of this report, provide to the Committee a detailed description of the steps the Intelligence Community is taking to increase analytic depth on the terrorist target. This description should include an assessment of the relative value of all current terrorist threat products; a determination, if any is required, as to whether new products would better serve the customers and which current products are insufficiently valuable and should be discontinued; and assignment of clear analytic responsibility to those who are tasked to produce terrorist threat products.

Recommendation #2: To the Director of Central Intelligence — Revise the existing procedures and standards for issuing formal Intelligence Community warning products. The revised system should include:

- a streamlined interagency coordination process;
- clear and concise standards for issuing warnings; and
- a system of threat ratings for the consumer, incorporating such factors as the immediacy, significance and reliability of the threat.

Create a training program for both the analysts involved in the terrorist threat warning process and the consumers of the warning products to ensure that they understand the standards for issuing a warning product and the significance of those products. Not later than 90 days after the receipt of this report, provide the Committee with a report on your progress in implementing this recommendation.

Chairman GOSS. I would now like to introduce the distinguished members of our panel today.

First, Senator Warren Rudman served in the Senate for two terms, from 1981 through 1992. Among other committee assignments, he chaired the Senate Select Committee on Ethics, was the Vice Chairman of the Senate Iran-Contra Committee and was a member of the Senate Intelligence Committee.

Since leaving the Senate, Senator Rudman has led commissions that have examined the U.S. Intelligence Community and emerging threats to the United States. Until December of 2001, he served as the Chairman of the President's Foreign Intelligence Advisory Board.

Senator, welcome.

Judge Louis Freeh served as Director of the FBI from September 1993 to June 2001. Prior to his service as FBI Director, he had a distinguished career as an FBI agent, Federal prosecutor, U.S. district court judge for the Southern District of New York.

Judge Freeh, welcome, sir.

Mary Jo White is the former U.S. attorney for the Southern District of New York. Her office prosecuted those responsible for the first attack on the World Trade Center, the plot against New York landmarks in 1993, the 1998 East Africa embassy bombings, as well as numerous other important cases of concern to this committee.

We welcome you, Ms. White. Thank you for joining us.

Dr. Paul Pillar is the National Intelligence Officer for the Near East and South Asia. Dr. Pillar has served in senior positions at the Central Intelligence Agency, including as the Deputy Chief of the DCI's Counterterrorist Center. He is the author of "Terrorism and U.S. foreign Policy." I would recommend that to anybody; as far as I am concerned, it is pretty close to the Bible and has served us well. Unfortunately, not enough people have read it apparently.

Dr. Pillar, welcome.

Each of our committees has adopted a supplemental rule for this Joint Inquiry that all witnesses shall be sworn. I will ask the witnesses to rise at this time.

I think, Mr. Fallis and Dr. Hoffman, I may as well ask you if you don't mind to rise and be sworn as well, just in case there are questions.

Thank you. We are missing Dr. Hoffman, I guess.

[Witnesses sworn.]

Chairman GOSS. The full statements of the witnesses will be placed in the record of these proceedings, as usual.

I will now call on Senator Rudman, then Judge Freeh, then Ms. White, and then Dr. Pillar, in that order, to give their opening spoken remarks.

Thank you. We welcome you all. We are truly delighted you are here.

Senator Rudman, the floor is yours, sir.

TESTIMONY OF THE HON. WARREN RUDMAN, FORMER UNITED STATES SENATOR FROM THE STATE OF NEW HAMPSHIRE

Mr. RUDMAN. Mr. Chairman, I am delighted to be here. This is the committee I served on, one of my favorite committees in my time in the Senate, and I am honored to appear before you.

I expect that two of the things that I did in the last few years are of interest to you and I have tried to draw from them in my testimony: first, of course, chairing PFIAB; secondly, chairing Hart-Rudman; and third, something I want to talk about a bit this morning that Chairman Goss is very familiar with, and that is the Roles and Other Responsibilities of the Intelligence Community for the 21st Century, which we prepared at the request of this Congress.

I think it is Public Law 971. I wish more people had read it. I want to talk a little bit about it this morning. I would highly recommend that every staff member read this before you write your final report, if you haven't already; and I would think that Members might want to read some portions of it, because it was a very distinguished group of Americans who spent a lot of time looking in advance of 9/11 at precisely the things that you are looking at post-9/11.

I want to just give you a couple of excerpts from that, and I will take 5 or 6 minutes. I do not have a prepared statement, but rather I thought I would respond to the specific questions addressed to me by the leadership of the committee.

The first question that you asked was that our national security study group, Hart-Rudman, warned in 2001 that the United States was not prepared to deal with terrorist attacks in the U.S. homeland. "Please summarize why you felt that to be true at the time, what steps were taken, if any, in response to our report and why we believe important steps were not taken and what measures remain to be taken."

Briefly, this Commission was commissioned by the Congress and the previous administration. Its task was to prepare a report on U.S. national security for the 21st century to be given to the incoming President in 2001, so no one knew who that would be at that time or what party that person would be in. It was a totally bipartisan group. We spent a huge amount of time. We traveled all over the world. We met with friend and foe. We met with intelligence agencies, those with whom we have good relations and those with whom we have poor relations.

And we came to the overwhelming conclusion at the end of our study that we were facing an asymmetric threat to our entire national security structure. And, to everyone's surprise, our lead recommendation dealt with homeland security and international terrorism.

No one on that committee would have thought at the time that we started that that would have been our conclusion. We would have thought it might have been more in the area of DOD reorganization or intelligence reorganization or changing the State Department, changing public diplomacy. It was not.

And you are all familiar with the report; I have discussed it with many of you personally. We said in that report, "More or less, large

numbers of Americans will die on American soil, victims of terrorism, in the coming century."

It happened a bit sooner, rather than later.

Why did we come to that conclusion? It was obvious. From the excellent history that Eleanor Hill gave you a few minutes ago, it was an escalation of attacks against American interests. It was quite apparent that the homeland was not secure and that, at a point in time, those terrorists, be it al-Qa'ida or many other groups—some of which you are, I am sure, studying; others which you may not be—that someone would launch an attack on this country.

We talked about weapons of mass destruction, we talked about weapons of mass disruption; and we laid it out in laborious detail, because it was overwhelmingly apparent to all of us that that was going to happen.

We made a number of recommendations. In late January 2001, we presented it to the new administration, to the National Security Advisor, the Vice President through the National Security Adviser and the President, the Secretary of State and the Secretary of Defense. It was very well received. People were very interested in it.

We brought it up here. We met with a number of you on this committee. To the credit of the Congress, a number of you immediately started moving towards a Homeland Security Department—which is now, I understand, wound up in some controversy, but I expect eventually it will happen—and we made a number of recommendations that Congress reacted very quickly to and started to act on them, particularly, in the House, Congressman Mac Thornberry; here in the Senate, Senator Fred Thompson and Senator Joe Lieberman.

The administration's attitude was, this is an excellent report, we are getting it to an internal task force of the NSC, and we will start to go through it. I find no fault in that. This is a brand new administration; it had much on its plate. It was the February-March time frame of 2001.

My understanding is that they were in the process of working on the recommendations. DOD, in fact, had done some of the things that we had recommended. So I would say that although people might criticize and say that the administration should have acted more forthrightly, my sense is, for a new administration receiving a voluminous report, including an implementation plan, they probably did about all that any administration would have done under the circumstances.

Let me also say that had every recommendation that we had put into that plan been adopted the day after we gave it to the White House, I seriously doubt that that would have been sufficient to prevent 9/11, for many reasons, including some of the reasons that your Staff Director has talked about here today.

Your second question: We said that military consumers often drove intelligence collection and that, given limited resources, the Community was neglecting important regions and trends. "How did this affect the ability of the United States to understand the growth of capabilities and locations such as Afghanistan and Yemen? Would placing more of the Intelligence Community under

the authority of the Director of Central Intelligence prevent similar problems in the future?"

The answer to your question is, generally yes. Up until September 11, the bulk of U.S. intelligence efforts had been focused on states. That has been the historic role of the United States Intelligence Community.

And I might add that our Intelligence Community, as well as most foreign ones that I have studied, are extraordinarily good at looking at structure, at capability, and intent. They don't have a very good track record even working against states for determining what and when; and I am not sure that that will ever be totally solved, no matter how hard we try.

To try to come up with a definition of people's intentions, whether they be states or they be shadowy terrorist organizations, is the toughest assignment given to any Intelligence Community; and frankly, if you look at the record over the last 50 years, the record is not particularly good, not here or anywhere else.

Do I believe, or did our Commission believe, in making the Director of the CIA, giving him a stronger role? We do, but we are not the first ones to say that. This has been recommended for many years.

You have a Director of Central Intelligence who is also the Director of CIA; 85 percent of that budget is controlled by DOD. From what I read in the papers lately, they would like to get even more control of it. And I leave that to you; you are elected to solve problems like that. I don't know what the answer is.

We have tried to recommend a number of reasonable solutions in this report, which a number of Members of Congress served on. Nothing has happened, except I do believe there is a stronger Community coordination effort since this report than there was before. But you have got a long way to go, and frankly, I think it is in the court of the Congress as much as it is the administration's.

We called for the President, through the NSC, to set strategic intelligence priorities and update them regularly. Was this done? Is it being done today?

I can tell you that I am no longer chairman of PFIAB, so I am no longer privy to those things, but my understanding is that, yes, there has been broad strategic intelligence directives, PDDs, which have been adopted by this administration. I am sure they would be available to this committee. I would advocate that you check with them to get a more precise answer.

Three more questions you asked:

"How can the United States improve cooperation between intelligence agencies focused overseas, CIA, NSA, et cetera, and those with domestic focus, such as the FBI; and how could they take full advantage of each other's capabilities? What gaps existed in their cooperation prior to September 11?"

I believe that the Joint Terrorism Centers, which these committees are very familiar with, have come a long way in cooperation; but we have got some very interesting issues here that have to do with law, civil rights, the rights of Americans.

I was saying to Louis Freeh before we testified this morning, that you go back and read the history of the 1946–1947 National Intelligence Act, and it was very clear that the FBI was responsible

for domestic counterintelligence, and I would expect counterterrorism; and the CIA was responsible overseas, and the CIA had better not come close to putting its nose anywhere near domestic issues. It was a wonderful alliance of strange bedfellows, J. Edgar Hoover and the American Civil Liberties Union.

They both had their precise reasons for feeling that way. But the result has been that we have not had the cooperation between these agencies that we should have. I think there ought to be major changes in the law. I have felt that way for a long time.

Let me add, just in response to one of the questions posed in one of the opening statements, to create a new MI5–type organization in this country, we did not believe on our Commission would be the solution. You have got enormous domestic collection capability in the FBI, assuming it is focused in the right direction. That is a tough issue and one this committee and the Judiciary Committee will have to work with.

"How effective do you believe that law enforcement tools are for fighting terrorism? Were they relied upon excessively before September 11?"

The answer to that, I guess, is yes and no.

Mary Jo White brought very successful prosecutions against a number of terrorist organizations in the Southern District of New York. On the other hand, President Bush says we are now at war. If we are at war, then law enforcement tools will be used, but in a more minor way; and military tools will be used more effectively to deal with the capability of terrorism. So I guess the answer to that question is both in the affirmative and in the negative.

Finally, "Any recommendations you may have for improving the Intelligence Community's performance in fighting terrorism."

I believe that the more jointness that you have between these agencies, the more they work in joint counterterrorism centers, the more their information databases become common, the more there is constant daily, hourly cooperation between them, the more that the NSA is brought in—by statute, if necessary—to supplying the FBI with domestic counterterrorism information, then you will do the improvement you need.

I do not believe we need new structures or new systems. We may need different kinds of people, we may need different kinds of technology, but I don't think there is anything wrong with the systems. I think there is a lot wrong with how they have been used over the last 10 years.

Finally, Mr. Chairman and members of the committee, I want to read to you from this report, which was submitted in 1996 to the Congress at the Congress' direction—as I said, Chairman Goss served on this and a number of other people that you all know; it was a very distinguished group—entitled "Commission on Roles and Capabilities of the United States Intelligence Community."

There are a lot of great recommendations in it. There is one here that is particularly interesting and it is from the executive summary. It is spelled out in detail, but I am not going to do that; I am just going to read you two paragraphs. It is entitled "The Need for a Coordinated Response to Global Crime."

"Global criminal activity carried out by foreign groups—terrorism, international drug trafficking, proliferation of weapons of

mass destruction and international organized crime—is likely to pose increasing dangers to the American people in the years ahead as perpetrators grow more sophisticated and take advantage of new technology. Law enforcement agencies historically have taken the lead in responding to these threats, but where U.S. security is threatened, strategies which employ diplomatic, economic, military or intelligence measures may be required instead of, or in collaboration with, law enforcement response. In the Commission's view, it is essential that there be overall direction and coordination of U.S. response to global crime."

I will tell you that nobody evidently read it.

Thank you, Mr. Chairman.

Chairman GOSS. Thank you very much, Senator Rudman, for obviously a very illuminating presentation to us.

We now go to Judge Freeh.

Welcome, sir. The floor is yours.

[The prepared statement of Judge Freeh follows:]

Statement of

Louis J. Freeh,

Former FBI Director,

before the

Joint Intelligence Committees

October 8, 2002

10:00 a.m.

INTRODUCTION

I want to begin by expressing my prayers and condolences for the victims, and to the Families and loved ones who have been devastated by terrorism, in all of its destructive forms. I spent 26 years in public service as an FBI Agent, prosecutor, Army Officer, judge and FBI Director, striving every day, as did my colleagues, to protect both people and the Rule of Law.

All who serve in law enforcement and public safety go to work every day committed to the possibility of laying down their lives to prevent harm to our fellow citizens. On September 11th, dozens of law enforcement officers, firefighters, and other brave people willingly did so. Special Agent Lenny Hatton and retired Special Agent John O'Neill unselfishly sacrificed their lives that day. John and Lenny represent the very finest of the FBI – men and women who I am immensely proud of and whose courage, skill, sacrifices and dedication in combating crime and terrorism, both here in this country and on the ground in far away dangerous places, deserve the nation's praise and enduring respect. It was a great and unique privilege to serve with these extraordinary Americans. We are sincerely thankful for Director Mueller's able leadership and for an FBI so dedicated to the people it serves.

I often had the occasion to work with John O'Neill. He was the FBI's counter-terrorism chief who helped forge what became the excellent and unprecedented FBI-CIA relationship in counter-terrorism. John and I stood together on the deck of the USS Cole in Aden harbor shortly after the October 2000 attack against our warship. We watched silently and reverently as young FBI Agents and technicians worked in the 110 degree hold of the devastated ship to carefully recover the remains of the 17 sailors killed in that brutal act of war against the United States. In June of 1996, John and I stood together in front of Khobar Towers in Saudi Arabia as hundreds of FBI men and women – again working in 120 degree temperatures – sifted through tons of debris removing human remains and evidence, intent on doing that which law enforcement can do when there is a terrorist act of war against America. In Dar es Salaam and Nairobi in August 1998 again I watched hundreds of FBI men and women sifting through the shattered ruins of our American embassies recovering human remains and evidence, all of us determined to bring to justice those who committed these atrocious acts against the United States of America.

In February 1993, I was sitting in my courtroom at Foley Square in downtown Manhattan when the World Trade Center was attacked by foreign, Al-Qaeda-trained terrorists. I walked from the courthouse and when I got to Chambers Street, I saw dozens of FBI Agents running down the street towards the smoke-filled building. My images and memories of these painful events are both horrific and heroic. The horror and suffering of the victims, balanced in a small but vital way, by the heroism, absolute focus and sacrifices of the rescuers and responders – and always, the incredible bravery and selflessness of the FBI employees, people who, like their colleagues, respond out of duty to their country.

It was amazing to me that this part of the scene was always the same. FBI men and women – whether it was New York City, Dhahran, Aden, Nairobi, Dar es Salaam – exhausted, many sick and dehydrated, working until they literally dropped in some cases, down on their knees digging with their hands and fingers, working in harms' way. In Yemen and East Africa, our Agents not only worked in extremely hazardous conditions, but had to be and were guarded round-the-clock by FAST teams of United States Marines to protect their lives as they pursued justice under the Rule of Law.

Another thing that has been a constant was the FBI's concern and support for the survivors of these horrendous acts. Their testimony in these cases speaks eloquently about the superb professionalism and dedication of the FBI's counter-terrorism people. The FBI men and women who have cared for and spent hundreds of hours comforting, informing and caring for these survivors are incredible. On numerous occasions, I visited with the surviving Families of the Americans killed in East Africa, on board the USS Cole and at Khobar Towers. We tried never to be too busy elsewhere that we stop pursuing the killers of their loved ones.

One of the most moving events in my years of public service was in June of 2001, days before I left the FBI, when all nineteen Families of the Khobar Towers victims came to my office and thanked me and the FBI for not forgetting about them – and for keeping our promise that the FBI would never stop its efforts to bring to justice the terrorists who killed their loved ones. I will treasure that moment forever.

As I said, it was an honor to work with men like John O'Neill, and the thousands of others, people like Dale Watson and Cofer Black – dedicated Americans for whose bravery, skill and absolute integrity America will always be thankful.

I would also like to commend President Bush and the Congress for their immediate responses in kind to the acts of those who are responsible for the events of September 11th. Even after my 26 years of public service, I was awestruck to see a united America exercise the will and might to carry out an all-inclusive, far-reaching and total war against terrorists who, from far away places, have threatened and attacked America for decades.

I would like to take a few minutes this morning to provide a broad overview of the terrorism threat and the FBI's role and history in fighting this evil. I would also like to focus on both the successes and the limitations of that mission prior to September 11th, important because the threats and needs for resources and authorities were the same on September 10th as they were on September 12th. I would also offer some ideas on strengthening and improving America's national security without weakening the foundation upon which our country has been built – governance under the Rule of Law.

OVERVIEW

EVERY ACT OF TERRORISM AROUND THE WORLD CANNOT BE PREVENTED

Terrorism has been waged against domestic, civil authority and invading armies for centuries. Its motivation and execution has unlimited variations over time and place. For that very reason and as a freedom loving people, we have to be careful about how we let terrorism be defined. It is inevitable that every act of terrorism cannot be prevented even under the best of circumstances. If reality was otherwise, some government or regime, using unlimited resources and unrestrained power, would have come up with a 100 percent preventive formula. America and other countries are fully capable of carrying out skillful, covert, highly compartmentalized and effective strikes against terrorists on the other side of the world. Our enemies from time-to-time are equally capable of such an attack against us, especially when they are anxious to die in the endeavor. No agency or country – particularly in a democracy where the Rule of Law is sacred – can be expected to foil and prevent every planned attack. Such a standard will never be met. Nevertheless, our law enforcement, our intelligence agencies, our political, economic, military and our diplomatic policies and efforts must strive to get as close to that 100 percent goal as humanly possible.

THE INTELLIGENCE COMMUNITY AND THE FBI DOES NOT APPEAR TO HAVE HAD SUFFICIENT INFORMATION TO PREVENT THE SEPTEMBER 11TH ATTACKS

What has been stated recently to this Committee by FBI Director Robert S. Mueller III includes the following:

> "The plans for the September 11th attacks "were hatched and financed overseas over a several year period.
>
> "Each of the hijackers, apparently purposely selected to avoid notice, came easily and lawfully from abroad ...
>
> "While here, the hijackers effectively operated without suspicion, triggering nothing that alerted law enforcement and doing nothing that exposed them to domestic coverage. As far as we know, they contacted no known terrorist sympathizers in the United States. They committed no crimes with the exception of minor traffic violations. They dressed and acted like Americans, shopping and eating at places like Wal-Mart and Pizza Hut. They came into different cities, moved around a lot and did not hold jobs. When three got speeding tickets in the days leading up to September 11, they remained calm and aroused no suspicion. One of the suicide hijackers, Nawaf al-Hazmi, even reported an attempted street robbery on May 1, 2001, to Fairfax, Virginia Police – he later declined to press charges.
>
> "None of the nineteen suicide hijackers are known to have had computers, laptops, or storage media of any kind, although they are known to have used publicly accessible Internet connections at various locations. They

used 133 different pre-paid calling cards to call from various pay phones, cell phones, and land lines.

"The nineteen suicide hijackers used U.S. checking accounts accessed with debit cards to conduct the majority of financial activity during the course of this conspiracy.

"Meetings and communications between the hijackers were done without detection, apparent surveillance flights were taken, and nothing illegal was detected through airport security screening.

"In short, the terrorists had managed very effectively to exploit loopholes and vulnerabilities in our systems. To this day we have found no one in the United States except the actual hijackers who knew of the plot and we have found nothing they did while in the United States that triggered a specific response about them."

We have read and heard much about the July 2001 memo by a Phoenix Special Agent, the Minnesota arrest and investigation of Moussaoui in August, and the information which the CIA obtained regarding two of the nineteen hijackers relating to a Kuala Lumpur meeting in 2000.

It is very important in hindsight to segregate this relevant information and put it into a dedicated timeline. However, the predictive value of these diverse facts at the time that they were being received must be evaluated. Analyzing intelligence information can be like trying to take a sip of water coming out of a fire hydrant. The several bits of information clearly connected and predictive after the fact need to be viewed in real time. The reality is that these unquestionably important bits have been plucked from a sea of thousands and thousands of such bits at the time. Additionally, as this Committee well knows, the difference between strategic and tactical intelligence is critically important to keep in mind.

Although not privy to all the relevant information known to this Committee, I am aware of nothing that to me demonstrates that the FBI and the intelligence community had the type of information or tactical intelligence which could have prevented September 11th. In terms of the FBI's capability to identify, investigate and prevent the nineteen hijackers from carrying out their attacks, the facts so far on the public record do not support the conclusion that these tragic events could have been prevented by the FBI and intelligence community acting by themselves. That is not to say things could not have been done better or that more resources or authorities would not have helped. It is only to say I have not seen a reporting of facts that leads to that conclusion, with one important caveat, however. Because of the narrow focus of this inquiry I leave aside any view of the larger but very relevant issues like foreign policy, military might, airline safety, national commitment, etc.

IDENTIFICATION, INVESTIGATION AND ARREST OF DANGEROUS TERRORISTS AND THOSE WHO SUPPORT THEM IS PREVENTION

For instance, the FBI's criminal investigation of the 1993 World Trade Center bombing led directly to the discovery and prosecution of a terrorist plot to blow up New York City tunnels, buildings, and infrastructure which would have killed thousands of innocent people. The FBI's investigation led to evidence and witnesses whose cooperation directly prevented a major terrorist attack. In my experience, the identification, pursuit and arrest of terrorists are the primary means of preventing terrorism. The FBI and CIA have jointly been doing this successfully for many years. Our investigation and pursuit of Ramzi Yousef after the World Trade Center bombing in 1993, let to the Philippines and helped to prevent his plot to blow up eleven United States airliners in the western Pacific. His arrest in Pakistan by FBI Agents certainly prevented him from carrying out further acts of terrorism against America. Bringing Yousef and the East Africa Embassy bombers back to the United States and convicting them in New York City without a doubt prevented them from carrying out more terrorism against America. As these Committees have known for several years, the FBI and the CIA have carried out joint operations around the world to disrupt, exploit and recover evidence on Al-Qaeda operatives who have targeted the United States. These operations, in part designed to obtain admissible evidence, also had the critical objectives of destroying the operational capability of terrorist organizations, collecting valuable intelligence and being able to support our military, should such a response be unleashed.

LAW ENFORCEMENT'S ABILITY TO ACT AGAINST ENTRENCHED TERRORISTS IN OVERSEAS SANTUARIES IS VERY LIMITED

The FBI and CIA can devise and implement a very effective counter-terrorism strategy both inside the United States and overseas. However, often a greater involvement of national resources is required. For example, General Noriega was investigated and indicted by the Department of Justice in 1988 operating out of what he thought was a safe, foreign haven. Noriega and his military-like organization were sending tons of deadly drugs into the United States, causing the deaths and devastation of countless Americans. The FBI and DEA built the case and executed the arrest warrant on Noriega in Panama only because our military can and did do what law enforcement and intelligence cannot. Usama Bin Laden was indicted in 1998, prior to Al-Qaeda's bombings of our two embassies in East Africa. Like Noriega, Usama Bin Laden remained secure and operational in his foreign, safe haven. Once the collective will to go in and get him was summoned, it happened with striking speed. The Pan Am 103 bombing is another such example of an FBI case where the Libyan intelligence service was the target of our investigation.

I certainly don't equate Noriega and Usama Bin Laden in terms of their destructiveness and evil. However, the comparison makes an obvious but often

overlooked point that our response to terrorism must be expansive, unmistakable, and unwavering across all levels of the United States Government

And I particularly want to commend George Tenet and the courageous men and women of the CIA for fighting bravely on the front lines of this war for many years. Under Mr. Tenet's sound leadership, dedication and vision, the CIA has achieved great successes in rolling-up major terrorist plots in Albania, Jordan, South East Asia and many other places. Importantly, the CIA and FBI have been fully cooperating and jointly carrying out America's counter-terrorism war for many years – forming the first joint FBI-CIA group dedicated to Al-Qaeda/Usama Bin Laden a year prior to the August 1998 East African embassy attacks.

But the fact is that working at their best and highest levels of efficiency and cooperation, the FBI and CIA together will still fall short of war a total war against terrorism.

As these Committees well know, total war – as we have recently done it – requires bold leadership supported by the will of Congress and the American people. Its success is ultimately dependent upon the united and unrelenting efforts of foreign policy, military assets, vast resources, legal authorities and international alliances and cooperation.

I realize that your Committees' efforts have publicly focused for the most part on the intelligence community and the FBI. And I'm confident that the upcoming Commission, should there be one, will more fully examine these broader issues with a global view. It should be obvious, for instance, that the FBI with about 3.5 percent of the country's counter-terrorism budget and the CIA with their share comprise but pieces of a mosaic of a total government commitment to the war on terrorism.

U.S. AIRLINES AND AVIATION HAVE LONG BEEN KNOWN AS A MAJOR TARGET FOR TERRORIST ATTACKS

Aviation and airplanes have long been known to be preferred targets of terrorist hijackers. Protecting civil aviation from a terrorist attack has for years been an urgent national issue. A September 1996 GAO Report concluded that "nearly every major aspect of the system ranging from the screening of passengers, checked and carry-on baggage, mail and cargo as well as access to secured areas within airports and aircraft – has weaknesses that terrorists could exploit."

In the aftermath of the tragedy of TWA Flight 800 in New York City, the White House Commission on Aviation Safety and Security was formed. I along with New York City Police Department Commissioner Ray Kelly, Bill Coleman, Franklin Raines, Jim Hall, and other distinguished Americans served as commissioners appointed by President Clinton. The Chairman of the Commission was Vice President Al Gore, who did an excellent job leading the effort and making much needed recommendations. Known as the Gore Commission, the panel made its final report and

recommendations on February 12, 1997. For example, Recommendation 3.19, entitled "Complement Technology with Automated Passenger Profiling", contemplated the development of a passenger profiling system wherein law enforcement and intelligence information on known or suspected terrorists would be used in passenger profiling.

The critical issue of terrorism directed against our aviation security was well known for many years prior to September 11th. As this Committee knows, the FBI conveyed repeated warnings to the FAA and the airline industry regarding terrorism, right up to September 11, 2001. Efforts by the government and the airline industry to implement these and other recommendations deserve intensive and careful study, and, most likely, massive resources.

This is not to criticize the FAA, which does a difficult job very well. Rather, the point is that while the CIA and the FBI should be intensely examined regarding September 11 – they should not be examined in a vacuum. The Executive and the Congress, the various government agencies with primary responsibility for public safety and national security, foreign policy, technologies, as well as the private sector and the international community are all components in whether or not terrorism is addressed with the vigor it so deserves.

RESOURCES

You have asked me to talk about resource allocation and whether sufficient resources were allocated to and within the FBI for fighting terrorism. The short answer is that the allocations were insufficient to maintain the critical growth and priority of the FBI's counter-terrorism program. The Gore Commission agreed when it recommended we "significantly increase the number of FBI Agents assigned to counter-terrorism investigations, to improve intelligence, and to crisis response."

In 1993, the FBI had under 600 Special Agents and 500 support positions funded for its entire counter-terrorism program, domestic and international alike. By 1999, that allocation had increased to around 1,300 Agents and a like amount of support positions. While at first blush that may sound like a lot, the FBI had requested significantly more counter-terrorism resources during this period. This was done because I had made the prevention, disruption and defeat of terrorism one of the FBI's highest priorities. We knew that many areas, like analysis and technology, needed huge influxes of new resources.

Let me read from the FBI's May 8, 1998 Strategic Plan, "The FBI has identified three general, functional areas that describe the threats which it must address to realize the goal of enhanced national and individual security:

- "TIER ONE: National and Economic Security – Foreign intelligence, terrorist and criminal activities that directly threaten the national or economic security of the United States. " (emphasis added)

* * * *

"These offenses fall almost exclusively within the jurisdiction of the FBI. Issues arising in this area are of such importance to U.S. national interests that they must receive priority attention. To succeed, we must develop and implement a proactive, nationally directed program."

- "Strategic Goal: Prevent, disrupt, and defeat terrorist operations before they occur.

  "Terrorism, is both international and domestic, poses arguably the most complex and difficult threat of any of the threats for which the FBI has a major responsibility. State-sponsored terrorism, though still of concern, is no longer the only terrorist problem. New perpetrators – loosely organized groups and ad hoc coalitions of foreigners motivated by perceived injustices, along with domestic groups and disgruntled individual American citizens – have attacked United States interests at home and abroad. They have chosen nontraditional targets and increasingly have employed nonconventional weapons. The dilemma, of course, is that the new perpetrators, targets, and weapons exist in almost unlimited numbers, while the law enforcement resources arrayed against them are finite." (emphasis added)

In my report to the American people on the work of the FBI 1993-1998, entitled "Ensuring Public Safety and National Security Under the Rule of Law", I wrote:

"One of my major priorities has been to seek increased funding for the FBI's counter-terrorism programs. The Congress has shown great foresight in strengthening this vital work. For example, the counter-terrorism budget for Fiscal Year 1996 was $97 million. The FY 1999 budget contains $301 million for counter-terrorism efforts."

* * * *

"Some terrorism now comes from abroad. Some terrorism is home-grown. But whatever its origin, terrorism is deadly and the FBI has no higher priority than to combat terrorism; to prevent it where possible; and where prevention fails, to apprehend the terrorists and to do everything within the law to work for conviction and the most severe sentences. Our goal is to prevent, detect and deter."

* * * *

"Foreign Terrorists in U.S.:"

"Terrorism can be carried out by U.S. citizens or by persons from other countries. At one time, with these crimes erupting in much of the world, many Americans felt we were immune from terrorism with foreign links. All of that ended in 1993." (emphasis added)

"The type of terrorism which had previously occurred far from our shores was brought home in a shocking manner when in February a massive explosion occurred in the parking garage at the World Trade Center complex in New York City."

The 1998-2000 period was critical and unprecedented regarding both the changes in and the demands on the FBI's Counter-Terrorism program and its domestic and international responsibilities.

As examples, we indicted Usama Bin Laden in June 1998 and again in November 1998. We put Bin Laden and Al-Qaeda on the FBI's Top Ten list, in April 1999, making them our number one Counter-Terrorism priority. Also in 1999, we set up a dedicated Usama Bin Laden Unit at FBI Headquarters.

We stood up for overseas deployment five Rapid Deployment Teams to respond to terrorist threats against America around the globe.

With help from Congress, we began to position ourselves around the globe in places that matter in the fight against terrorism. Without those FBI Legats, the post-September 11th advances could never had been made with such speed and surety.

We doubled and tripled the number of Joint Terrorism Task Forces (JTTFs) around the United States so we could multiply our forces and coordinate intelligence and Counter-Terrorism operations with the FBI's federal, state and local law enforcement partners. Thirty-four of these JTTF's were in operation by 2001.

The FBI was given national responsibility for coordinating the protection of the Nation's critical infrastructure. As a result, we created the National Infrastructure Protection Center (NIPC) at FBI Headquarters which had critical responsibilities regarding terrorist threats and cyberattacks.

The FBI was also tasked to set up the National Domestic Preparedness Office to counter terrorist threats and to enhance homeland security.

We began making preparations for the 2000 Olympics, the Millennium, United Nations and NATO meetings in New York City, World Cup, IMF-World Bank events, presidential conventions and other major special events which absorbed vast numbers of FBI Counter-Terrorism resources.

At the same time, we were conducting major terrorism investigations leading up to the successful prosecution in New York City of the Al-Qaeda members who attacked our embassies in Africa.

We stood up the massive Strategic Information Operations Center (SIOC) at FBI Headquarters whose main purpose was to give us the capability to work several major and simultaneous terrorist matters at the same time.

We established the FBI's Counter-Terrorism Center at FBI Headquarters which was coordinated with the CIA's Center by communications, information exchange, and personnel staffing.

We instituted MAX CAP O5 in July 2000 to enable each of the FBI's 56 Field Offices and their Special Agents in Charge (SAC) to improve our counter-terrorism efforts, analyze threats and develop capabilities and strategies throughout the United States. Regional SAC Conferences were held during the summer of 2000 to roll out the MAX CAP O5 strategy.

We set up a national threat warning system in order to disseminate terrorism-related information to state and local authorities around the country.

We organized and carried out a significant number of national, regional and local practical exercises to help the country prepare for terrorist attacks.

The Attorney General and I conducted regular meetings with the National Security Advisor and the Secretary of State dedicated to terrorism issues, cases and threats.

I met with dozens of Presidents, Prime Ministers, Kings, Emirs, law enforcement, intelligence and security chiefs around the world. The primary reason for these contacts was to pursue and enhance the FBI's counter-terrorism program by forging an international network of cooperation. We were not an island. It had to be done.

We proposed and briefly received from Congress the authority to hire critical scientists, linguists and computer specialists without the salary restrictions of Title V. This flexibility is critical to fighting terrorism.

The DOJ and the FBI prepared hundreds of FISA Court applications in counter-terrorism matters where electronic surveillance or legal assistance was required from the Court.

I regularly met and discussed counter-terrorism issues, intelligence and force protection issues with the Attorney General, the National Security Advisor, United

States Attorneys, the Secretaries of State and Defense, our Ambassadors and the Joint Chiefs of Staff.

Perhaps, most significantly as to the issue of the FBI's focus on the terrorist threat, in November 1999, I created a new FBI Counter-Terrorism Division. Nobody in the Executive or the Congress suggested that this step be taken. I took it because I firmly believed that it was necessary to expand and enhance the FBI's counter-terrorism capability. Dale Watson was elevated to run this new Division and develop our new strategies. We enhanced and reorganized the entire FBI Counter-Terrorism Program.

At the same time, I proposed the creation of a new, Investigative Services Division to support the new Counter-Terrorism Division as well as the Criminal and National Security Divisions. My purpose in doing so was to put together all of the FBI's analytical and support assets in order to better prevent terrorism and enhance our intelligence bases with the resources that we had available.

Nine months later, this reorganization was approved and the FBI for the first time consolidated its counter-terrorism program assets with the support of a greater analytical engine. Ultimately, history has shown that more was needed on every front, ours included.

In February 2001, we held a National Counter-Terrorism Conference to roll out details of the MAX CAP 05 strategy to counter the terrorist threat.

The 2000, 2001 and 2002 (pre September 11, 2001) budgets fell far short of the counter-terrorism resources we knew were necessary to do the best job. This is not meant as a criticism but a reminder for the record that total war against terrorists was not the same priority before September 11th as it is today.

Here are the numbers:

For FYs 2000, 2001 and 2002 FBI counter-terrorism budgets, I asked for a total of 1,895 Special Agents, analysts, linguists and others. The final, enacted allocation I received was 76 people over those three years. For example, in FY 2000 I requested 864 additional counter-terrorism people at a cost of $380.8 million. I received 5 people funded for $7.4 million.

Thus, at the most critical time, the available resources for counter-terrorism did not address the known critical needs.

By contrast, in response to the FBI's FY 2002 Emergency Supplemental request for additional counter-terrorism-related resources, Congress enacted 823 positions for $745 million, all things which we needed prior to September 11th.

A final note on FBI resources to carry out its critical mission, including waging war against terrorists: To win a war it takes soldiers. Front line troops, as you know, each require several more soldiers to support them. I don't know if the Joint Staff has advised you, but even after September 11th, the FBI has less FBI Agents today – 11, 516 Special Agents – than it had in 1999 – when the number was 11,681. By way of comparison, in 1992, before I became Director, the FBI had 10,479 – that's only 1,037 less than today – an average, annual growth of about 103 Special Agents per year over the last decade. We also must keep in mind that these 11,516 Special Agents have responsibility for other immensely important and resource-consuming programs including new jobs regularly imposed by Congress without additional resources.

With less FBI Agents than the Chicago Police Department has sworn officers, the immensely important responsibilities of the FBI are not proportionally represented in its most basic resource – soldiers.

I would urge you to significantly increase the personnel of the FBI and to favorably consider pending legislation that would more fairly compensate them for the life-saving work they do every day.

Further, it is critical that we fully support and protect our FBI Agents and CIA Officers. One example how we could do this better can be found in a recommendation by the National Commission on Terrorism. It noted:

> "The risk of personal liability arising from actions taken in an official capacity discourages law enforcement and intelligence personnel from taking bold actions to combat terrorism."
>
> "FBI Special Agents and CIA Officers are buying personal liability insurance, which provides for private representation in such suits. By recent statute, federal agencies must reimburse up to one half of the cost of personal liability insurance to law enforcement officers and managers or supervisors."

We need to support the brave men and women whom we ask to take great risks for our nation's safety.

THE FBI WAS FOCUSED BOTH ON PREVENTING DOMESTIC AND FOREIGN TERRORIST ATTACKS

As I stated earlier and as reflected in the FBI's 1998 Strategic Plan and Five-Year Report, the 1993 bombing of the World Trade Center by foreign terrorists clearly demonstrated the effort to target America and Americans. Usama Bin Laden's fatwah calling for the deaths of Americans anywhere left no doubt that terrorist attacks within the United States were as likely as those in Saudi Arabia, East Africa, Yemen and elsewhere.

More convincingly, the failed efforts by Ressam and his New York City-based co-conspirators to carry out a major terrorist attack within the United States at the end of 1999 made the FBI focus intently on protecting homeland security. Indeed, the FBI investigation of the USS Cole attack and CIA efforts overseas led to our conclusion that the millennium attacks by Ressam on the West Coast were planned to coincide with other Al-Qaeda sponsored terrorism in Jordan and in Yemen. The Jordanian attack was prevented by the CIA acting together with the Jordanian General Intelligence Service (GIS) to stop it. The Al-Qaeda suicide bombers of the USS Cole had previously planned to attack another United States warship – The USS Sullivans – which was docked at the same fuel pod the USS Cole used in October 2000. The earlier attack was postponed because the bomb-laden attack boat sunk when it was launched.

So before the end of 1999, the FBI and the intelligence community clearly understood the foreign-based Al-Qaeda threat regarding targets within the United States. Congress and the Executive were fully briefed as to this threat analysis.

In several appearances before this Committee, I used a chart to depict the locations around the United States where radical fundamentalists cells were active. The FBI fought unsuccessfully to continue fingerprinting and photographing visiting nationals from key state-sponsors of terrorism states because of our concern that intelligence agents were being sent here to support these radical elements.

The notion that the FBI, other law enforcement agencies and the intelligence community were not focused on homeland threats is not accurate and belied by many factors. For example, as we prepared for and conducted the several, major trials of Al-Qaeda members – Usama Bin Laden was charged as a defendant in those indictments – in New York City, during 1999-2000, extraordinary security steps were taken to prevent an Al-Qaeda attack. If any of you saw Foley Square, the federal courthouse and the area around City Hall, 26 Federal Plaza and the New York Police Department Headquarters during this time, it was totally fortified. The closed streets, cement trucks, barricades, checkpoints and hundreds of heavily armed officers and agents were not set up to prevent the Al-Qaeda subjects from escaping. These unprecedented security measures – enhanced after September 11 – were designed to stop Al-Qaeda attacking the court which found their own members guilty of blowing up our embassies in Africa.

Similarly, Pennsylvania Avenue was ordered closed by the National Security Advisor and the White House after the United States Secret Service Director and I made a presentation which showed that a terrorist vehicle bomb could destroy the West Wing.

Prior to September 11, an incredible number of innovative and costly measures were regularly implemented by the FBI and the law enforcement community around the country – at special events, conventions, inaugurations, public gatherings – to prevent, among other threats, foreign based terrorists like Ressam and Yousef from

attacking targets here. The radical fundamentalist threat posed a clear and present danger here and everyone knew it and understood it to be the case.

At the same time, the FBI was critically active in focusing on the terrorist threat to Americans overseas. Much of that activity I have recounted above. Beginning in 1993, shortly after I became Director, I determined that to protect America at home, the FBI needed to significantly increase its international role and liaison with our foreign law enforcement and security counterparts. I determined that to have an effective counter-terrorism program that protected Americans in their homes and offices, the FBI had to have its Agents in Cairo, Islamabad, Tel Aviv, Ankara, Riyadh, and other critical locations around the world. We opened FBI Legat Offices in those countries to strengthen our counter-terrorism program. The critical alliances and partnerships with the law enforcement and security services in those countries has paid enormous benefits and has protected this nation and our people from acts of terrorism.

We later were able to open FBI Legat offices in Amman, Almaty, New Delhi and when I left the FBI in June 2001, I had pending requests to establish FBI offices in thirteen additional countries, having already more than doubled the FBI presence overseas from 19 to 44. I was pleased recently to learn that my prior requests to open offices in Tunis, Kuala Lumpur, Tbilisi, Sana and Abu Dhabi had been approved. The FBI must have this foreign presence and capability to carry out an effective counter-terrorism policy, especially when it comes to prevention.

When I left the FBI, I had proposed that we establish an FBI training facility in Central Asia, as we had done in Budapest in 1996, and had begun in Dubai, to enhance our ability to establish liaison and critical points of contact in those important regions. There is absolutely no substitute for these liaisons and relationships. Without them we risk being blind.

Many FBI personnel and I spent an enormous amount of time traveling overseas in order to establish an international counter-terrorism capability. Because of that, in 1998, I was able to negotiate the return of two Al-Qaeda bombers from Kenya so they could be tried and convicted for the embassy bombings.

In 2000 I met with President Musharraf in Pakistan and negotiated the availability of a critical witness in one of our major terrorist prosecutions in New York. I briefed him on the indictment against Bin Laden on the 1998 embassy bombings and asked for his assistance in capturing him. FBI Agents and a prosecutor from the United States Attorney's Office-Southern District of New York later returned to Pakistan to continue these efforts.

In 1996, I met with Presidents Nazarbayev and Karimov of Kazakhstan and Uzbekistan, respectively, and discussed radical fundamentalist terrorism directed against the United States from Afghanistan and Iran. I asked for their help in fighting these threats to America as well as to them.

I traveled extensively – as did scores of FBI men and women – throughout the Mideast, Central Asia, Africa, Asia, the Persian Gulf and South America with the objective of strengthening the FBI's counter-terrorism program so we could better protect America.

Dozens of FBI Special Agents went to places like the Triborder Area in South America, South East Asia, Africa, Greece, Georgia, Russia and many other places to carry out the FBI's counter-terrorism mission.

History and experience have shown that the FBI's expansion overseas has paid immense dividends in terms of enhanced capability, prevention and enforcement.

For example, our examination of the forensic evidence from the USS Cole case, we discovered that the explosive used was possibly manufactured in Russia. Because the FBI had been working in Russia since 1994, I was able to call the FSB Director and ask for assistance. His response was immediate. Russian explosive experts provided the FBI with all the necessary forensic and expert information requested, helping the case immensely. I could provide dozens of other examples of how the FBI's expanded Legat Program has directly supported our efforts to protect America from terrorists.

THE 1996 KHOBAR BOMBING INVESTIGATION DEMONSTRATES THE FBI'S SUCCESSES AND LIMITATIONS IN COMBATING FOREIGN-BASED TERRORISTS WHO WAGE WAR AGAINST THE UNITED STATES

The FBI's 1996 Khobar bombing investigation is a prime example of the FBI's success in combating terrorism because of solid relationships with our foreign partners. It also points to the limitations in dealing with these acts strictly as criminal cases. After that devastating terrorist attack on June 25, 1996, which killed 19 United States Airmen and wounded hundreds more, the FBI was instructed to mount a full-scale criminal investigation. We immediately dispatched several hundred FBI personnel to Dhahran, Saudi Arabia, and, supported by the armed forces, established a crime scene, interviewed available witnesses, obtained evidence and set out leads and an investigative plan.

Working in close cooperation with the White House, State Department, CIA and Department of Defense, I made a series of trips to Saudi Arabia in order to further the FBI's investigation. Because the FBI's prior contacts with the Saudi police service, the Mabaheth, and Interior Ministry had been carried on from offices Rome and, later, Cairo, the FBI lacked any effective liaison or relationship with its counterpart agencies in Riyadh.

Fortunately, the FBI was able to forge an effective working relationship with the Saudi police and Interior Ministry. After several trips and meetings with the Saudi leadership and particularly, Prince Nayef, the Interior Minister, the FBI was

granted permission to expand its presence and joint, operational capability within the Kingdom. I was particularly fortunate to gain the trust and cooperation of Prince Bandar bin Sultan, the Saudi Ambassador to the United States who was critical in achieving the FBI's investigative objectives in the Khobar case. Due to Prince Bandar's forthcoming support and personal efforts, the FBI was able to establish an FBI office in Riyadh. Our Arabic-speaking Special Agent who became the first FBI Agent to be assigned to Saudi Arabia quickly made critical liaison and relationships of trust were established between the FBI and the Mabaheth. Evidence and access to important witnesses were obtained and excellent investigative support was furnished to various teams of FBI Agents who worked in Saudi Arabia to pursue the case. In one instance, Canadian authorities, acting on Saudi information, arrested a Khobar subject who was brought to the United States and thereafter sent by the Attorney General to Saudi Arabia for prosecution.

The cooperation the FBI received as a result of Princes Bandar and Nayef's personal intervention and support was unprecedented and invaluable. From time-to-time a roadblock or legal obstacle would occur which was expected given the marked differences between our legal and procedural systems. Despite these challenges, the problems were always solved by the personal intervention of Prince Bandar and his consistent support for the FBI.

The case almost faltered on the issue of the FBI's critical request for direct access to six Saudi nationals who were being detained in the Kingdom and who had admitted participation in the Khobar bombing. One of these subjects, who had been returned to Saudi Arabia from another country, had key information which would later implicate senior Iranian government officials as responsible for the planning, funding and execution of this attack. We needed direct access to these subjects because their admissions and testimony were critical to support our prosecution. Yet no FBI Agent had ever been given such unprecedented access to a detained Saudi national, which access could potentially taint their prosecution under Islamic law. Moreover, by making these witnesses directly available to the FBI, the Saudis understood that they would be helping to provide evidence that senior officials of the government of Iran were responsible for the Khobar attack.

Despite these extremely sensitive and complex issues, the Saudis put their own interests aside to aid the FBI and the United States. Supported by Prince Bandar, Prince Nayef and the Saudi Mabaheth, Crown Prince Abdullah decided to grant the FBI's request to interview the detainees. Ambassador Wyche Fowler worked closely with me in this endeavor and finally we succeeded. Teams of FBI investigators then were able to have access to these critical detainees and full debriefings were conducted in Saudi Arabia. As a direct result of these and later direct interviews, the Department of Justice was able to return a criminal indictment in June 2001, charging thirteen defendants with the murders of our nineteen servicemen. The indictment was returned just days before the statute of limitations would have run on some of the criminal charges. This case could not have been made without the critical support and active assistance of Saudi Arabia and the State Department through Ambassador Fowler.

The direct evidence obtained strongly indicated that the 1996 bombing was sanctioned, funded and directed by senior officials of the government of Iran. The Ministry of Intelligence and Security (MOIS) and Iranian Revolutionary Guard Corps (IRGC) were shown to be culpable for carrying out the operation. The bombers were trained by Iranians in the Bakka Valley. Unfortunately, the indicted subjects who are not in custody remain fugitives, some of whom are believed to be in Iran.

Khobar represented a national security threat far beyond the capability or authority of the FBI or Department of Justice to address. Neither the FBI Director nor the Attorney General could or should decide America's response to such a grave threat. While on the one hand, Khobar demonstrated the capability of the FBI, acting in cooperation with its foreign counterparts overseas, to work successfully under extremely complex conditions to pursue criminal cases; it also demonstrated that an act of war against the United States – whether committed by a terrorist organization or by a foreign state – can receive only a limited response by the FBI making a criminal case against those harbored beyond the reach of law enforcement.

Mr. Watson recounted a meeting that he and I had with you, Senator Shelby, and Senator Bob Kerry. We came up to brief you on the Khobar attack and how the FBI's investigation was proceeding. You both very correctly told me that while it was necessary for the FBI to go to Yemen and collect the facts, an attack upon our warship was an act of war, much graver than merely a horrific crime.

I never lost sight of that fact and its truth is even more apparent after September 11th. The FBI always viewed these investigations as secondary to any national security action and severely limited in their overall impact on a far away enemy such as Al-Qaeda. I always stressed that the FBI investigations were completely secondary to the needs of our national security.

The National Commission on Terrorism made this point convincingly by using the pursuit of the Pan Am 103 case – investigated by the FBI – as an example of the more aggressive, national strategy needed against this scale of terrorism:

> "Law enforcement is designed to put individuals behind bars, but is not a particularly useful tool for addressing actions by states. The Pan Am 103 case demonstrates the advantages and limitations of the law enforcement approach to achieve national security objectives. The effort to seek extradition of the two intelligence operatives implicated most directly in the bombing gained international support for economic sanctions that a more political approach may have failed to achieve. The sanctions and the resulting isolation of Libya may have contributed to the reduction of Libya's terrorist activities. On the other hand, prosecuting and punishing two low-level operatives for an act almost certainly directed by Qadafi is a hollow victory, particularly if the trial results in his implicit exoneration."

The Commission concluded that "Iran remains the most active state supporter of terrorism ... the IRGC and MOIS have continued to be involved in the planning and execution of terrorist acts. They also provide funding, training, weapons, logistical resources, and guidance to a variety of terrorist groups ... including Lebanese Hizballah ... Hamas ... PIJ ... and PFLP-GC." The Commission noted that "In October 1999, President Clinton officially requested cooperation from Iran in the investigation [of the Khobar bombing]. Thus far, Iran has not responded. International pressure in the Pan Am 103 case ultimately succeeded in getting some degree of cooperation from Libya. The United States Government has not sought similar multilateral action to bring pressure on Iran to cooperate in the Khobar Towers bombing investigation."

We must always recognize the limitations inherent in a law enforcement response. As we see at this very moment in history, others, to include Congress, must decide if our national will dictates a fuller response.

MODERN INFORMATION TECHNOLOGY IS NECESSARY TO COMBAT TERRORISM

When I left office in June 2001, the FBI was just beginning to get back on track in upgrading its information technology. In fact, just one month prior to my departure, the FBI was finally able to award the first contract for the Trilogy initiative, a three-year program to upgrade the FBI's aging information technology infrastructure.

I can't underscore how important IT is to the ability of the FBI to combat terrorism, in particular, and in performing all aspects of its national security, criminal investigative, and law enforcement assistance missions. The FBI's problem with acquiring necessary information technology has a long history. We didn't just wake up one day and realize that our IT systems were unable to perform even basic functions, such as e-mail and electronic files that were available in other government agencies and the private sector. Indeed, upgrading FBI IT was one of the three areas – along with training and analytical capacities – identified in the FBI Strategic Plan issued in March 1998 as being most critical to the success of the FBI.

To address our IT shortfalls, the FBI proposed a five-year IT technology upgrade plan, called the Information Sharing Initiative (ISI). That initiative would have allowed the FBI to replace outdated desktop computers, upgrade network capacity to permit the exchange of images and other large files, provide improved analytical capabilities, and permit information sharing with other law enforcement, prosecutorial, and intelligence agencies. The initial planning behind the ISI project began as early as 1992. The FBI estimated the cost of the ISI project to be approximately $432 million. Through the budget process, we began requesting the additional funding needed to proceed with ISI; at the same time, we pursued a parallel contract competition so that we would be in a position to award a contract when funding became available.

The project consisted of three phases: internal information sharing, analytical tools and intelligence processing, and external information sharing. Most of the initial effort was aimed at replacing existing, outdated and obsolete equipment with up-to-date desktop computers, higher capacity servers and mainframe computers; acquiring standardized off-the-shelf office automation software for word processing and spreadsheets; acquiring more robust telecommunication circuits and networks that could handle larger image, text, and audio files; and, implementing commercially available analytical tools to improve our intelligence capabilities.

There was some development work involved, primarily in the later stages of the project where existing FBI databases would migrate from older databases applications to a new enterprise relational database that would permit word and phrase searching not possible under the existing ACS platform. Some development would also have been required for building external information sharing capabilities. The risk in this latter area involved developing necessary layered security protocols and "trusted guards" so authorized non-FBI personnel could access those parts of our databases they were cleared to, while at the same time preventing unauthorized access to sensitive FBI information.

Our first budget proposal to the Congress for ISI was in 1998 as part of the Fiscal Year 1999 appropriations request. We sought a total of $70 million for ISI, consisting of $20 million from base IT funding and an increase of $50 million in new budget authority for ISI. Congress appropriated $2 million of the requested increase, to be used for additional personnel to support ISI, and directed the Attorney General to make available $40 million from the Department's Working Capital Fund. However, Congress prohibited the FBI from spending any of these funds, including the $20 million from the FBI's base IT budget, until a comprehensive implementation plan was submitted to the Congress.

During the FY 2000 appropriations cycle, we proposed a total of $58.8 million for ISI, consisting of $20 million from base IT funding and an increase of $38.8 million in new budget authority. The FY 2000 appropriation for the FBI provided no new budget authority and again prohibited the FBI from obligating any available funds for ISI until the Congress approved the ISI plan.

After receiving Administration clearance, the FBI submitted the ISI plan to the Congress in March 1999; however, the plan was not accepted. A revised plan was submitted in August 1999. Still, this plan was not approved. We continued to talk with the Congress and we presented alternate funding scenarios, but we could not reach agreement. There was universal agreement that the FBI needed the IT upgrade requested; however, there was disagreement on the type of contract vehicle being proposed, how much the FBI could or should do using in-house capabilities versus contractors, deployment to field offices, staging of the capabilities within each phase, and cost.

While awaiting approval of the ISI plans, the FBI had extended the bids submitted for the ISI contract. However, it became necessary to cancel the procurement in November 1999 due to our inability to reach agreement and release of funding for ISI.

Due to the restrictions on spending any funds for ISI, the FBI was precluded for a two year period from replacing or upgrading many elements of it's IT infrastructure since these items were encompassed by the ISI plan. This was particularly damaging since $40 million of the embargoed funds were funds from our base IT budget that were normally used for basic refreshment and upgrades of existing equipment and systems. Desktop computers grew older and more obsolete; network switches, servers, and other equipment become more fragile and more prone to breakdown.

We came back to the Congress in the FY 2001 budget with a request for a total of $60 million in funding for FBI information technology infrastructure upgrades, consisting of $20 million from base IT funds and $40 million in new budget authority. In March 2000, we also submitted yet another plan, entitled, e-FBI: Three Year Implementation Plan, Architecture, Schedule, Cost, and Program Management Details. This plan was built around a Congressionally suggested funding stream of $200 million, or half the amount initially proposed by the FBI for ISI.

In early 2000, I recruited Bob Dies, who had recently retired from IBM, to come in and rework our proposal in an effort to break the impasse that developed between the FBI and the Congress modernizing the FBI's IT infrastructure. Subsequently, in September 2000, Mr. Dies submitted to the Congress a revised investment plan, entitled, FBI Technology Upgrade Plan, Reprioritized Three-Year Implementation Plan. That plan called for spending a total of $380 million to upgrade the FBI's information technology infrastructure, or some $52 million less than the original ISI proposal.

The new plan was built around three components: information presentation, transportation network, and user applications. Congressional clearance for the new plan came in September 2000 and the FBI was allowed to spend $100.7 million for first year costs of the plan. That $100.7 million consisted of the $80 million that was banked from FYs 1999 and 2000, plus $20.7 million from base IT funding. Contracts for the Trilogy program, as the revised plan became known, were finally awarded in May and June 2001.

The last FBI budget proposal that I presented to the Congress – for FY 2002 – included a request for $67.7 million for the second year costs of the Trilogy program. I am pleased that the Congress provided the full amount needed for year two Trilogy costs and, in subsequent supplemental appropriations, provided even more funding for Trilogy and other FBI IT investments.

CRITICAL TECHNOLOGY ASSISTANCE IS REQUIRED TO FIGHT THE WAR AGAINST TERRORISM

In addition to IT, other critical technology assistance is required for the FBI to continue an effective war against terrorism.

In 1994, as a result of the FBI's own initiative, Congress passed the Communications Assistance to Law Enforcement Act (CALEA). This critical statute was vital to ensuring that law enforcement could maintain the technical ability to conduct court-authorized electronic surveillance. Against tremendous opposition, the FBI persuaded Congress that this selectively-utilized technique was essential to working its most complex criminal and national security cases. Support from Chairman Leahy, Senator Hatch and many other members was critical in this legislation. The law simply allows the FBI to continue its court-controlled use of this capacity as the telecommunications world changes from an analog to digital network. It has taken most of the last eight years to fund and to implement CALEA and faster progress needs to be made.

But CALEA simply permits the FBI to maintain court-approved access to digital communications and stored data. Another technical challenge called encryption then and now threatens to make court-authorized interception orders a nullity. Robust and commercially available encryption products are proliferating and no legal means has been provided to law enforcement to deal with this problem, as was recently done by Parliament in the United Kingdom. Terrorists, drug traffickers and criminals have been able to exploit this huge vulnerability in our public safety matrix.

Many of you have heard me and others testify before you about this problem for many years. The International Association of Chiefs of Police (IACP), the fifty State Attorneys General, and National Association of District Attorneys have all identified this problem as the most critical technology issue facing law enforcement. Many of you, Chairman Goss, Representative Norm Dicks, Senators Kyl and Feinstein have provided outstanding leadership and gone to great lengths to address this problem. In 1998, HPSCI adopted a substitute bill to S.909 which effectively addressed all of law enforcement's public safety and terrorism-related concerns regarding encryption products. Unfortunately, this needed counter-terrorism assistance was not enacted. As we know from Ramzi Yousef's encrypted computer files found in Manila, terrorists are exploring this technology to defeat our most sophisticated methods to prevent their attacks. I have long said that this unaddressed problem creates a huge vulnerability in our nation's counter-terrorism program. Neither the Patriot Act nor any other likely-to-be-enacted statute even attempts to close this gap. Resolving this issue is critical to homeland security.

In 1995, Congress authorized the FBI to establish a Technical Support Center. The purpose of this facility was to provide federal and local law enforcement with the technical tools to improve court-authorized telecommunication interceptions

and signal access for investigative purposes. I was pleased to see that this critical center was fully funded subsequent to September 11th.

Many other critical technology needs must be addressed both with legal authorization – such as the once-proposed Cyberspace Electronic Security Act (CESA) bill – and significant new resources for counterterrorism, cyberterrorism and dealing with weapons of mass destruction and proliferation threats.

The convergence of technology and globalization now enable an individual terrorist or a small group of terrorists, operating from the other side of the world in a protected sanctuary, to threaten our nation in devastating ways.

WE NEED TO ACKNOWLEDGE THAT THE RULES GOVERNING THE FBI'S COUNTERTERRORISM EFFORTS CHANGED AS A RESULT OF SEPTEMBER 11TH

We must acknowledge that the rules are changed beginning with certain provisions of the USA Patriot Act. The Department of Justice and the intelligence agencies have been given new tools to combat a dangerous enemy who follows no rules. Some of these new authorities have been granted by the Congress with a sunset provision. Some asserted by the government are being challenged in the courts, where they will ultimately be decided.

It must always be understood that prior to September 11th, the FBI – as it always must – followed the rules as they were given to us by the Attorney General and the Congress. For example, FBI Agents were not permitted without special circumstances to visit a suspect group's web site or to attend its public meetings. Counterintelligence, Domestic Terrorism and Informant Guidelines promulgated years ago and updated with new restrictions curtailed our ability to collect information in national security cases. Those guidelines are now being changed. "Primary purpose" requirements for FISA applications and information separation structures limited the sharing of criminal and intelligence information. Grand jury and Title III secrecy provisions severely restricted the dissemination of criminal terrorist information obtained during those processes.

I repeatedly testified before Congress that FBI Agents were statutorily barred from obtaining portions of credit reports on certain national security subjects which used car dealers could order and read.

Before we interviewed detained foreign national Al-Qaeda members in East Africa in connection with the embassy bombings, FBI Agents gave them their Miranda rights.

And when I left the FBI in June 2001, we were being criticized in some quarters because a valuable new electronic tool necessary to read a terrorist's e-mail pursuant to a court order had the hypothetical potential to be abused – as any law enforcement tool could be.

Everyone understands why and how some of the rules changed after September 11th. But it is important to understand that the rules were changed by changed circumstances and that those circumstances changed the standards and expectations of both the FBI and CIA.

THE FBI AND CIA HAVE FULLY COOPERATED AND WORKED SIDE-BY-SIDE FIGHTING TERRORISM

During my tenure as FBI Director, I was immensely proud of the cooperation and integration of FBI and CIA efforts to combat terrorism. Myself and recent DCIs, particularly George Tenet, have taken bold and unprecedented steps to work together and forge an effective FBI-CIA partnership to combat terrorism. Exchanging senior officers, standing up the joint Usama Bin Laden/Al-Qaeda operations and intelligence center, fully coordinating our Legat and Station Chiefs, cross-training and many additional measures were taken to integrate our counter-terrorism resources and capabilities. Our joint efforts in the East Africa bombings is a template for how successful we were in working together. Some of these efforts cannot be described in this session.

This historical and successful integration does not mean that on every possible point of intersection, a lapse did not occur. But to focus on those isolated instances while ignoring the huge successes of this top-down directed integration, is misplaced. I personally credit George Tenet with making this happen and winning the trust and respect of the entire FBI in the process.

The best confirmation of this fully integrated FBI-CIA counterterrorism effort is the fact that during my tenure no chairman or member of these Committees raised with me – or the DCI to my knowledge – the issue of our agencies being uncooperative or adverse to working together. Conversely, it was repeatedly pointed out to me by your Committees that the FBI and CIA were working together in an exemplary manner.

SOME RECOMMENDATIONS

1. Provide legal authority and significant new funding enabling the FBI to manage encryption technology.

2. Significantly increase the number of FBI Special Agent and Support positions with sufficient compensation required to recruit and retain the best men and women to combat terrorism.

3. Significantly increase the FBI's technical support program and facilitate the FBI's access to emerging technologies and research and development by the private sector.

4. Significantly increase the number and staffing of FBI Legat Offices overseas.

5. Exempt the FBI from the compensation restrictions of Title V.

6. Change the FBI's procurement procedures to facilitate the efficient design and acquisition of equipment and technology.

7. Provide new funding for the FBI's international training programs and put the FBI in charge of all international law enforcement training.

8. Fund whatever it takes to achieve interoperability between all the agencies engaged in the war against terrorism.

9. Restructure the budget to give more flexibility to the DCI, Attorney General and the FBI Director to better allocate program funding and resources as missions evolve and new threats emerge.

10. Consider establishing a domestic public safety office in the Executive with responsibility for coordinating and supporting national law enforcement issues.

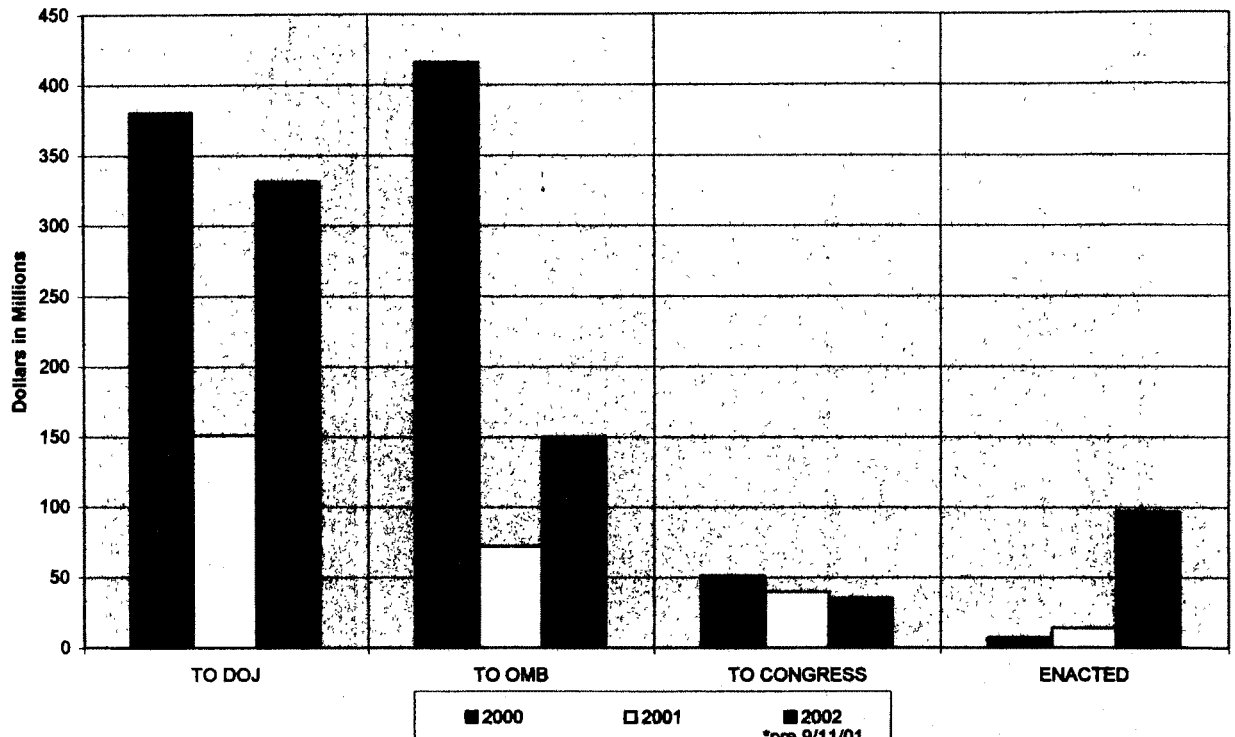
11. Enhance the legal, technical and funding resources of the FBI rather than consider creating an intelligence agency to share its domestic, pubic safety responsibilities.

CONCLUSION

The FBI and CIA working together have accomplished much in fighting terrorism at home and abroad but it is a constant and continuing battle. These agencies should remain the primary counterterrorism agencies for this mission. The DCI's authority for coordinating and implementing government-wide efforts in this regard should be expanded. The war against terrorism must be waged relentlessly. It will require that significantly more resources be allocated to the FBI and CIA. These fine agencies and the brave men and women who fight this war cannot defeat some forms of terrorism without total government intervention no matter how great and heroic their efforts. Al-Qaeda-type organizations, state sponsors of terrorism like Iran, and the threats they pose to America are beyond the competence of the FBI and the CIA to address. America must maintain the will in some cases to use its political, military and economic power in response when acts of war are threatened or committed against our nation by terrorists or their state sponsors.

Finally, however treacherous the enemy, the FBI must fight this war as a law enforcement agency of the Department of Justice governed by the Rule of Law and the Constitution. The rules, statutes and guidelines which establish the legal authorities of the FBI may change – as they did after September 11th – as long as those changes are clearly defined and understood. Its adherence to the Constitution and the Rule of Law must not change. We do not have sacrifice our freedom to protect it.

FBI Requests for Additional Counterterrorism-related Resources



TESTIMONY OF THE HON. LOUIS FREEH, FORMER DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Judge FREEH. Thank you, Mr. Chairman, Chairman Graham, members of the committee; thank you very much for inviting me to testify here today.

When I went back and recounted all the appearances that I have made before the Congress, the first one actually was in 1980 before Senator Rudman when I was an FBI agent. But other than that, I have appeared before these two committees more than all the other committees to which the FBI Director reports; and I think that is symbolic, one, of the attention that this committee and the bipartisan leadership, which I always have commended and commend today, has taken up the issues of national security and particularly counterterrorism.

Some of those hearings were requested by the committee. Some were requested by myself. And this committee, over the years, has been outstanding in its support and its thinking ahead, for the issues that we needed to deal with.

I would ask the committee's indulgence for what I will try to do in a summary fashion, but which I think is going to take some more time than I had planned.

First of all, I would like to begin by expressing my condolences to the victims of not just the horrific events of September 11, but all the victims of terrorism. And in the 26 years that I have spent as an FBI agent, an Army officer, a prosecutor, and a judge, I have strived every day, as have my colleagues, to ensure that the people that we were required to protect were protected to the best of our ability.

I would like to say here a few words about the men and women in law enforcement, and I know how much they are appreciated by this committee, but I know I speak this morning to a larger audience. All of those who serve in law enforcement and public safety go to work every day committed to laying down their lives for the people that they protect. On September 11, dozens of law enforcement officers, firefighters, other brave people willingly did so.

FBI Special Agent Lenny Hatton and retired FBI Special Agent John O'Neill unselfishly sacrificed their lives that day. John and Lenny represent the very finest of the FBI, men and women of whom I am immensely proud of and whose courage, skill, sacrifices, and dedication in combating crime and terrorism, both here in this country and on the ground in faraway, dangerous places, deserves the Nation's praise and enduring respect. It was a great and unique privilege to serve with these extraordinary Americans; and we are sincerely thankful for Director Mueller's able leadership and for the FBI, so dedicated to the people it serves.

I often had occasion to work with John O'Neill. He was, as you know, the FBI's Counterterrorism Chief, who helped forge the historical relationship, the positive relationship between the FBI and the CIA, about which I would like to say a few words.

John and I stood together on the deck of the USS *Cole* in Aden shortly after the October 2000 attack against our warship. As we stood there, we watched young FBI agents reverently remove the remains of those 17 sailors from the hull of the ship, and it was about 110 degrees. We watched silently and reverently as this was

done, and observed what was indeed an act of war against the United States.

In June of 1996, John and I stood together in front of Khobar Towers in Saudi Arabia as hundreds of FBI men and women working in 120-degree temperatures sifted through tons of debris, removing human remains and evidence, intent on doing that which law enforcement can do when there is an act of war committed against America.

In Dar es Salaam and Nairobi, in August of 1998, again I watched hundreds of FBI men and women sifting through the shattered ruins of our embassies, recovering human remains and evidence, all of us determined to bring to justice those who had committed these acts of war against the United States.

In February, 1993, I was sitting in my courtroom in Foley Square when the World Trade Tower was attacked by foreign al-Qa'ida-trained terrorists. I walked quickly from the courthouse. When I got to Chambers Street, I saw dozens and dozens of FBI agents streaming out of their building down the street towards the smoke-filled building.

My images and memories of these painful events are both horrific and heroic, the horror and suffering of the victims balanced in a small but vital way by the bravery and heroism of the rescuers. It was amazing to me that this part of the scene was always the same: FBI men and women—whether it was New York City, Dhahran, Aden, Nairobi, Dar es Salaam—exhausted, many sick and dehydrated, working until they literally dropped in some cases, down on their knees digging with their fingers, working in harm's way.

In Yemen and East Africa to do that work, they had to be surrounded 24 hours by fast teams of U.S. marines to protect their lives, and all the time working, pursuing justice under the rule of law.

Another thing that has been a constant was the FBI's concern and support for the survivors of these horrendous acts. Their testimony in these cases speaks eloquently about the superb professionalism and dedication of the FBI's counterterrorism men and women. They have cared for and spent hundreds of hours comforting, informing, and caring for these survivors.

On numerous occasions I visited with the surviving families of the Americans killed in East Africa, on board the USS *Cole,* and at Khobar Towers. We try never to be too busy elsewhere that we stop pursuing the killers of their loved ones.

One of the most moving events in my years of public service was in June of 2001, days before I left the FBI, when all 19 families of the Khobar Towers victims came to my office and thanked me and the FBI for not forgetting about them.

As I said, it was an honor to work with men like John O'Neill, thousands of others, people whom you know well—Dale Watson, Cofer Black, dedicated Americans for whose bravery, skill and absolute integrity America will always be thankful.

I would also like to commend President Bush and the Congress for their immediate responses, in kind, to the acts of those who are responsible for the events of September 11.

Even after my 26 years of public service, I was awestruck to see a united America exercise the will and might to carry out an all-exclusive, far-reaching and total war against terrorists who, from far away sanctuaries, have threatened and attacked America for decades.

I would like to take a few minutes this morning to provide a broad overview of the terrorism threat and the FBI's role in history in fighting it. I would also like to focus on both the successes and limitations of that mission prior to September 11, important because I think the threats and needs for resources and authorities were the same on September 10 as they were on September 12. I would also offer some ideas for strengthening and improving our national security without weakening the foundation upon which our country has been built—governance under the rule of law.

Terrorism has been waged against us and others for centuries. It is inevitable, and it's a sad fact that it is, that every act of terrorism cannot be prevented under the best of circumstances. If reality were otherwise, some government or regime using unlimited resources and unrestrained power would have come up with a 100 percent preventive formula. Our enemies from time to time are equally capable of an attack against us, especially when they are anxious to die in the endeavor.

No agency or country, particularly in a democracy where the rule of law is respected, can be expected to foil and prevent every planned attack. Such a standard will never be met. Nevertheless, our law enforcement, our intelligence agencies, our political, economic, military and our diplomatic policies must strive to get as close to that 100 percent goal as humanly possible.

The Intelligence Community and the FBI, in my opinion, does not appear to have had sufficient information to prevent the September 11 attacks.

What has been stated recently to this committee, in closed session I believe and later released, was a statement by FBI Director Mueller. I would like to repeat an excerpt of it; he testified before you as follows:

"The plans for the September 11 attacks were hatched and financed overseas over a several-year period. Each of the hijackers, apparently purposely selected to avoid notice, came easily and lawfully from abroad.

"While here, the hijackers effectively operated without suspicion, triggering nothing that alerted law enforcement and doing nothing that exposed them to domestic coverage. As far as we know, they contacted no known terrorist sympathizers in the United States. They committed no crimes with the exception of minor traffic violations. They dressed and acted like Americans, shopping and eating at places like Wal-Mart and Pizza Hut.

"They came into different cities, moved around a lot, did not hold jobs. When three got speeding tickets in the days heading up to September 11, they remained calm and aroused no suspicion. One of the suicide hijackers, Nawaf al-Hazmi, even reported an attempted street robbery on May 1, 2001, to Fairfax, Virginia, police. He later declined to press charges.

"None of the 13 suicide hijackers are known to have had computers, laptops, or storage media of any kind, although they are

known to have used publicly accessible Internet connections at various locations. They used 133 different prepaid calling cards to call from various pay phones, cell phones, and land lines.

"The 19 suicide hijackers used U.S. checking accounts accessed with debit cards to conduct the majority of financial activity during the course of this conspiracy. Meetings and communications between the hijackers were done without detection, apparent surveillance flights were taken and nothing illegal was detected through airport security screening.

"In short, the terrorists had managed very effectively to exploit loopholes and vulnerabilities in our system. To this day, we have found no one in the United States except the actual hijackers who knew of the plot, and we have found nothing they did while in the United States that triggered a specific response about them."

We have read and heard much about the July 2001 memo by a Phoenix special agent, the Minnesota arrest and investigation of Moussaoui in August, and the information which the CIA obtained regarding two of the 19 hijackers relating to Kuala Lumpur meeting in 2000. It is very important, in hindsight, to segregate this relevant information and put it into a dedicated time line. However, the predictive value of these diverse facts at the time that they were being received must be evaluated.

Analyzing intelligence information can be like trying to take a sip of water coming out of a fire hydrant. The several bits of information clearly connected and predictive after the fact need to be viewed in real time. The reality is that these unquestionably important bits have been plucked from a sea of thousands and thousands of such bits at the time. Additionally, as this committee well knows, the difference between strategic and tactical intelligence is critically important to keep in mind.

Although not privy to all the relevant information known to this committee, I am aware of nothing that to me demonstrates that the FBI and the Intelligence Community had the type of information or tactical intelligence which could have prevented the horror of September 11. In terms of the FBI's capability to identify, investigate, and prevent 19 hijackers from carrying out their attacks, the facts so far in the public record do not support the conclusion that these tragic events could have been prevented by the FBI and Intelligence Community acting by themselves.

This is not to say things could have been done better or that more resources or authorities would not have helped. It is only to say I have not seen a reporting of facts that leads to that conclusion, with one important caveat: Because of the narrow focus of this inquiry, I leave aside any view of the larger, but very relevant issues raised even this morning by Eleanor Hill, like foreign policy, military might, airline safety, national commitment.

Identification, investigation and arrest of dangerous terrorists and those who support them is prevention. I would like to try to dispel the notion that investigation is not part of prevention. I think Mary Jo White will speak about that a little bit.

For instance, the FBI's criminal investigation of the 1993 World Trade Tower bombing led directly to the discovery and prosecution of a terrorist plot to blow up New York City tunnels, buildings and infrastructure which would have killed thousands of innocent peo-

ple. The FBI's investigation at that time led to evidence and witnesses whose cooperation directly prevented a major terrorist attack.

In my experience, the identification, pursuit and arrest of terrorists are the primary means of preventing terrorism in some cases. The FBI and CIA have jointly been doing this successfully for many years. Our investigation and pursuit of Ramzi Yousef after the World Trade Center bombing in 1993 led to the Philippines and helped to prevent his plot to blow up 11 United States airliners in the Western Pacific.

His arrest in Pakistan by FBI agents certainly prevented him from carrying out further acts of terrorism against America. Bringing Yousef and the East Africa embassy bombers back to the United States and convicting them in New York City without a doubt prevented them from carrying out more terrorism against America.

As these committees have known for several years, the FBI and CIA have carried out joint operations around the world to disrupt, exploit and recover evidence on al-Qa'ida operatives who have targeted the United States. These operations, in part designed to obtain admissible evidence, also have the critical objectives of destroying the operational capability of terrorist organizations, collecting valuable intelligence and being able to support our military should such a response be unleashed.

Law enforcement's ability to act against entrenched terrorists in overseas sanctuaries is very limited. And I'll repeat here, in theme, another point made by your counsel this morning. The FBI and CIA can devise and implement a very effective counterterrorism strategy both inside the United States and overseas. However, often a greater involvement of national resources is required.

For instance, General Noriega was investigated and indicted by the Department of Justice in 1988 operating out of what he thought was a safe foreign haven. Noriega and his military-like organization were sending tons of deadly drugs into the United States, causing the deaths and devastation of countless Americans. The FBI and DEA built a case and executed the arrest warrant on Noriega in Panama only because our military can and did do what law enforcement and intelligence cannot do. Usama bin Ladin was indicted in 1998, actually prior to al-Qa-ida's bombings of our embassies in East Africa. Like Noriega, Usama bin Ladin remains secure in and operational in his foreign safe haven. Once the collective will to go in and get him was summoned, it happened with striking speed.

The Pan Am 103 bombing is another such example of an FBI case where the Libyan intelligence service was the target of our investigation.

I certainly don't equate Noriega and Usama bin Ladin in terms of their destructiveness or evil. However, the comparison makes an obvious but often overlooked point that our response to terrorism must be expansive, unmistakable, and unwavering across all levels of the United States Government.

I particularly want to commend George Tenet and the courageous men and women of the CIA for fighting bravely on the front lines of this war for many years. Under Mr. Tenet's sound leader-

ship, dedication, and vision, the CIA has achieved great successes in holding up major terrorist plots in Albania, Jordan, Southeast Asia many other places. Importantly, CIA and FBI have been fully cooperating and jointly carrying out America's counterterrorism war for many years.

And I will make this point again and again this morning: The coordination between the FBI and the CIA in counterterrorism in my eight years of experience has been exemplary.

They formed, the FBI and the CIA, the first joint dedicated al-Qa'ida-Usama bin Ladin cell, to study it, a year prior to the August, 1998, East African embassy bombings. But the fact is that, working at their best and highest levels of efficiency and cooperation, the FBI and CIA together will fall short of war, a total war against terrorism.

As these committees well know, total war, as we have recently done it, requires bold leadership supported by the will of Congress and the American people. Its success is ultimately dependent upon the united and unrelenting efforts of foreign policy, military assets, vast resources, legal authorities, and international alliances and cooperation.

I realize that your committee's efforts have been publicly focused for the most part on the Intelligence Community and the FBI. And I'm confident that the upcoming commission, should there be one, will more fully examine these broader issues with a global view. It should be obvious, for instance, that the FBI, with about 3.5 percent of the country's counterterrorism budget, and the CIA with their share comprise but pieces of a mosaic of a total government commitment needed to fight the war on terrorism.

For instance, U.S. airlines and aviation have long been known as a major target for terrorist attacks. I've cited in my statement a 1996 GAO report which concluded, "Nearly every make or aspect of the system, ranging from the screening of passengers, checked and carry-on baggage, mail and cargo, as well as access to secured areas within airports and aircraft, has weaknesses that terrorists could exploit."

In the aftermath of the tragedy of TWA flight 800 in New York City, the White House Commission on Aviation Safety and Security was formed. Along with New York City Police Department Commissioner Ray Kelly, Bill Coleman, Franklin Raines, Jim Hall and other distinguished Americans served as Commissioners, appointed by President Clinton. The Chairman of the Commission was Vice President Al Gore, who did an excellent job leading the effort and making much-needed recommendations. Known as the Gore Commission, the panel made its final report and recommendations on February 12, 1997. For example, in recommendation 3.19, entitled "Complement Technology with Automated Passenger Profiling," this contemplated the development of a passenger profiling system wherein law enforcement and intelligence information on known or suspected terrorists would be used in passenger profiling.

The critical issue of terrorism directed against our aviation security was well known for many years prior to September 11. As this committee knows, the FBI conveyed repeated warnings to the FAA and the airline industry regarding terrorism right up to September 11, 2001. Efforts by the government and airline industry to imple-

ment these and other recommendations deserve intensive and careful study and, most likely, massive resources.

This is not to criticize the FAA, which does a difficult job very well. Rather, the point is that while the CIA and the FBI should be intensely examined regarding September 11, they should not be examined in a vacuum. The executive and the Congress, the various government agencies with primary responsibility for public safety and national security, foreign policy, technologies, as well as the private sector and the international community are always components in whether or not terrorism is addressed with the vigor it deserves.

You've asked me to talk about resource allocation and whether sufficient resources were allocated to and within the FBI for fighting terrorism. The short answer is that the allocations were insufficient to maintain the critical growth and priority of the FBI's counterterrorism program. The Gore Commission agreed when it recommended "that we significantly increase the number of FBI agents assigned to counterterrorism investigations to improve intelligence and to crisis response."

In 1993, the FBI had under 600 special agents and 500 support positions funded for its entire counterterrorism program, domestic and international. By 1999, that allocation had increased to about 1,300 agents and a like amount of support positions. While, at first blush, that may sound like a lot, the FBI had requested significantly more counterterrorism resources during this period; and I note for the record that this committee supported those recommendations as best it could.

This was done because I had made the prevention, disruption, and defeat of terrorism one of the FBI's highest priorities. We knew that many areas, like analysis and technology, needed huge influxes of new resources. Let me read from our May 8, 1998, strategic plan. "The FBI has identified three general functional areas that describe the threats which it must address to realize the goal of enhanced national individual security:

"Tier One: National and economic security—foreign intelligence, terrorist and criminal activities that directly threaten the national and economic security of the United States.

"These offenses fall almost exclusively within the jurisdiction of the FBI. Issues arising in this area are of such importance to U.S. national interests that they must receive priority attention. To succeed, we must develop and implement a proactive nationally directed program.

"Strategic goal: Prevent, disrupt and defeat terrorism operations before they occur.

"Terrorism, both international and domestic, poses arguably the most complex and difficult threat of any of the threats for which the FBI has a major responsibility. New perpetrators, loosely organized groups and ad hoc coalitions of foreigners motivated by perceived injustices, along with domestic groups and disgruntled American citizens have attacked United States interests at home and abroad. They have chosen nontraditional targets and increasingly have employed nonconventional weapons. The dilemma, of course, is that the new perpetrators, targets, and weapons exist in

almost unlimited numbers, while the law enforcement resources against them are finite."

In my report to the American people on the work of the FBI 1993–1998 entitled "Ensuring Public Safety and National Security Under the Rule of Law," I wrote, "One of my major priorities has been to seek increased funding for the FBI's counterterrorism programs. The Congress has shown great foresight in strengthening this vital work. For example, the counterterrorism budget for fiscal year 1996 was $97 million. The fiscal year 1999 budget contains $301 million for counterterrorism efforts."

"Some terrorism now comes from abroad. Some terrorism is home-grown. But whatever its origin, terrorism is deadly and the FBI has no higher priority than to combat terrorism, to prevent it where possible. Our goal is to prevent, detect and deter.

"Foreign terrorists in the United States," and a lot of this goes to the point of whether we were focused on domestic threats, domestic threats from terrorists:

"Terrorism can be carried out by U.S. citizens or by persons from other countries. At one time, with these crimes erupting in much of the world, many Americans felt we were immune from terrorism with foreign links. All that ended in 1993.

"The type of terrorism which had previously occurred far from our shores was brought home in a shocking manner when, in February, a massive explosion occurred in the parking garage at the World Trade Center complex in New York City."

The 1998–2000 period was critical and unprecedented regarding both the changes in and the demands on the FBI's counterterrorism program and its domestic and international responsibilities.

As examples, we indicted Usama bin Ladin in June of 1998 and again in November 1998. We put bin Ladin and al-Qa'ida on the FBI Top Ten list in April of 1999, making them our number one counterterrorism priority. Also in 1999, we set up a dedicated Usama bin Ladin unit at FBI's headquarters.

We stood up for overseas deployment five Rapid Deployment Teams to respond to terrorist threats against America around the world.

With help from Congress, we began to position ourselves around the globe in places that matter in the fight against terrorism. Without our FBI Legats, the post-September 11 advances could never have been made with such speed and surety.

We doubled and tripled the number of Joint Terrorism Task Forces around the United States so we could multiply our forces and coordinate intelligence and counterterrorism operations with the FBI's Federal, State, and local law enforcement partners. Thirty-four of these JTTFs were in operation by 2001.

The FBI was also given national responsibility for coordinating the protection of the Nation's critical infrastructure. As a result, we created the National Infrastructure Protection Center at FBI headquarters, which had critical responsibilities regarding terrorist threats and cyberattacks.

We were also tasked to set up the National Domestic Preparedness Office to counter terrorist threats and to enhance homeland security.

We began making preparations for the 2000 Olympics, the Millennium, United Nations and NATO meetings in New York City, World Cup, IMF-World Bank events, Presidential conventions and other major events, which absorbed vast numbers of FBI counterterrorism resources.

At the same time, we were conducting major terrorism investigations leading up to the successful prosecution in New York City of the al-Qa'ida members who attacked our embassies in Africa. We stood up the massive Strategic Information Operations Center at FBI headquarters whose main purpose was to give us the capability to work several major and simultaneous terrorist matters at the same time.

We established the FBI's Counterterrorism Center at FBI Headquarters, which was coordinated with the CIA's Center by communications, information exchange, and personnel staffing.

Chairman GOSS. Mr. Freeh, may I interrupt for a moment. Members have been notified by bells that we have a vote in the House. I understand there's a 15-minute vote followed by two 5-minutes. The 15-minute vote has probably eight or nine minutes left on it. We will be excusing ourselves to run over and make those votes, but I understand we will continue on and Chairman Graham will be taking over. Excuse me for the interruption, sir.

Judge FREEH. Thank you, Mr. Chairman.

Chairman GRAHAM [presiding]. Thank you, Mr. Freeh. Continue, please.

Judge FREEH. We instituted MAX CAP 05 in July, 2000, to enable each of the FBI's 56 field offices and their Special Agents in Charge to improve our counterterrorism efforts, analyze threats and develop capabilities and strategies throughout the United States. Regional SAC conferences were held during the summer of 2000 to roll out the MAX CAP 05 strategy.

We set up a national threat warning system in order to disseminate terrorism-related information to State and local authorities around the country.

We organized and carried out a significant number of national, regional and local practice exercises to help the country prepare for terrorist attacks.

The Attorney General and I conducted regular meetings with the National Security Advisor and the Secretary of State dedicated to terrorism issues, cases and threats.

I met with dozens of Presidents, Prime Ministers, Kings, Emirs, law enforcement, intelligence and security chiefs around the world. The primary reason for these contacts was to pursue and enhance our counterterrorism program by forging an international network of cooperation.

We proposed and briefly received from the Congress the authority to hire critical scientists, linguists and computer specialists without the salary restrictions of Title V.

The Department of Justice and the FBI prepared hundreds of FISA court applications in counterterrorism matters.

I regularly met with and discussed counterterrorism issues, intelligence and force protection issues with the Attorney General, the National Security Adviser, United States Attorneys, the Secretaries

of Defense and State, our Ambassadors and the Joint Chiefs of Staff.

Perhaps most significantly, as to the issue of our focus on the terrorist threat, in November of 1999, I created a new FBI Counterterrorism Division. Nobody in the executive or the Congress suggested that this step be taken; I took it because I firmly believed it was necessary to expand and enhance the FBI's counterterrorism capability. Dale Watson was elevated to run this new division and develop new strategies.

At the same time, I proposed the creation of a new Investigative Services Division to support the new Counterterrorism Division, as well as the Criminal and National Security Divisions. My purpose in doing so was to put together all of the FBI's analytical and support assets in order to better prevent terrorism and enhance our intelligence bases with the resources we had available.

Nine months later, this reorganization was approved and the FBI for the first time consolidated its counterterrorism program assets with the support of a greater analytical engine.

In February 2001, we held a National Counterterrorism Conference to roll out details of the MAX CAP 05 strategy.

The 2000, 2001 and 2002, pre-September 11, budgets fell far short of the counterterrorism resources we knew were necessary to do the best job. This is not meant as a criticism, but a reminder for the record that total war against terrorists was not the same—was not the same priority before September 11 as it is today.

Here are the numbers: For fiscal years 2000, 2001 and 2002, FBI counterterrorism budgets, I asked for a total of 1,895 Special Agents, analysts, linguists and others. The final, enacted allocation we received was 76 people over those 3 years. For example, in fiscal year 2000, I requested 864 additional counterterrorism people at a cost of $380.8 million; I received five people funded for $7.4 million.

Thus, at the most critical time, the available resources for counterterrorism did not address the known critical needs.

By contrast, in response to the FBI's fiscal year 2002 emergency supplemental request for counterterrorism-related resources, Congress enacted 823 positions and $745 million in new funding, all things which we needed prior to September 11.

A final note on FBI resources to carry out its critical mission, including waging war against terrorists. To win a war, it takes soldiers. Frontline troops, as you know, each require several more to support them. I don't know if your staff has advised you, but even after September 11, the FBI has less FBI agents today—11,516 Special Agents—than it had in 1999, when the number was 11,681.

By way of comparison, in 1992, before I became Director, the FBI had 10,479. That's only 1,037 less than today, an average annual growth of about 103 Special Agents per year over the last decade.

We must also keep in mind that these 11,516 Special Agents have responsibility for other immensely important and resource-consuming programs, including new jobs readily imposed by Congress without any additional resources.

With less FBI agents than the Chicago Police Department has sworn officers, the immensely important responsibilities of the FBI are not proportionately represented in its most basic resource, sol-

diers. Again, this is not by way of criticism. I do not think that, at the time, the national priority existed for the resources that are needed for this critical need, and I hope that they do now.

I would urge you to significantly increase the personnel of the FBI and to favorably consider penning legislation that would more fairly compensate them for the life-saving work they do every day.

Further, it's critical that we fully support and demonstrate that support for our FBI agents and CIA officers. One example of how we could do this better can be found in a recommendation by the National Commission on Terrorism. It noted, "The risk of personal liability arising from actions taken in an official capacity discourages law enforcement and intelligence personnel from taking bold actions to combat terrorism. FBI Special Agents and CIA officers are buying personal liability insurance which provides for private representation in some suits. By recent statute, Federal agencies must reimburse up to one-half of the cost of personal liability insurance for law enforcement officers and managers or supervisors." We need to support the brave men and women whom we ask to take great risk for us every day.

The FBI was focused both on preventing domestic and foreign terrorist attacks. I take exception to the finding that we were not sufficiently paying attention to terrorism at home.

As I stated earlier and as reflected in the strategic report and the 5-year report, the 1993 bombing of the World Trade Center by foreign terrorists clearly demonstrated the effort to target America and Americans. Usama bin Ladin's 1998 fatwa calling for the deaths of Americans anywhere left no doubt that terrorist attacks within the United States were as likely as those in Saudi Arabia, East Africa, Yemen and elsewhere.

More convincingly, the failed efforts by Ressam and his New York City-based coconspirators to carry out a major terrorist attack in the United States at the end of 1999 made the FBI focus intently on protecting homeland security. Indeed, the FBI investigation of the USS COLE attack and CIA efforts overseas led to our conclusion that the Millennium attacks by Ressam on the West Coast were planned to coincide with other al-Qa'ida-sponsored attacks in Jordan and Yemen. The Jordanian attack was prevented by the CIA acting together with the Jordanian intelligence service.

The al-Qa'ida suicide bombers of the USS *Cole* had previously planned to attack another U.S. warship, the USS *The Sullivans,* which was docked at the same fuel pod the USS *Cole* used in October, 2000. The earlier attack was postponed only because the bomb-laden attack boat sunk when it was launched.

So, before the end of 1999, the FBI and the Intelligence Community clearly understood the foreign-based al-Qa'ida threat regarding targets within the United States. Congress and the executive were fully briefed as to this threat analysis, particularly the leadership and membership of these committees in hearings and briefings—two, three calls late at night and over the weekend were continuously apprised of this threat.

In several appearances before this committee, I used a chart to depict the locations around the United States where radical fundamental cells were active. The FBI fought unsuccessfully to continue fingerprinting and photographing visiting nationals from key state

sponsors of terrorism states because of our concern that intelligence agents were being sent here to support these radical elements within America.

The notion that the FBI, other law enforcement agencies, the Department of Justice, and the Intelligence Community were not focused on homeland threats is not accurate and belied by many factors. For example, as we prepared for and conducted the several major trials of al-Qa'ida members—Usama bin Ladin, remember, was charged as a defendant in those indictments—in New York City during 1999–2000, extraordinary security steps were taken to prevent an al-Qa'ida attack. If any of you saw Foley Square, the Federal courthouse and the area around City Hall, 26 Federal Plaza, and the New York Police Department Headquarters during that time, it was totally fortified. The closed streets, cement trucks, barricades, checkpoints and hundreds of heavily armed officers and agents were not set up to prevent the al-Qa'ida subjects from escaping from the courthouse. These unprecedented security measures, enhanced after September 11, were designed to stop al-Qa'ida attacking the court which found their own members guilty of blowing up our embassies in Africa.

Similarly, Pennsylvania Avenue was ordered closed by the National Security Adviser and the White House after the United States Secret Service Director and I made a presentation which showed that a terrorist vehicle bomb could destroy the West Wing.

Prior to September 11, an incredible number of innovative and costly measures were regularly implemented by the FBI and the law enforcement community around the country—at special events, conventions, inaugurations, public gatherings—to prevent, among other threats, foreign-based terrorists like Ressam and Yousef from attacking targets here. The radical fundamentalist threat posed a clear and present danger here, and everyone knew and understood it to be the case.

At the same time, the FBI was critically focused and active regarding the terrorist threat to Americans overseas. Much of that activity I have recounted above. Beginning in 1993, shortly after I became Director, I determined that to protect America at home, the FBI needed to significantly increase its international role and liaison with our foreign law enforcement and security counterparts.

I determined, to have an effective counterterrorism program that protected Americans in their homes and offices, the FBI had to have its agents in Cairo, Islamabad, Tel Aviv, Ankara, Riyadh and other critical locations around the world. We opened FBI Legat offices in those countries to strengthen our counterterrorism program. The critical alliances and partnerships with the law enforcement and security services in those countries has paid enormous benefits and has protected this nation and our people from acts of terrorism.

We later were able to open FBI Legat offices in Amman, Almaty, New Delhi. When I left the FBI in June of '01 I had pending requests to establish FBI offices in 13 additional countries, having already more than doubled the FBI presence overseas. I was pleased recently to learn that my prior request to open offices in Tunis, Kuala Lumpur, Tbilisi, Sanaa and Abu Dhabi have been approved.

The FBI must have this foreign presence and capability to have an effective counterterrorism policy.

When I left the FBI, I proposed that we establish an FBI training facility in Central Asia, as we had done in Budapest in 1996 and had begun in Dubai, to enhance our ability to establish liaison and critical points of contacts in those regions. Many FBI personnel and I spent an enormous amount of time traveling overseas in order to establish an international counterterrorism capability. Because of that, in 1998, I was able to negotiate the return of two al-Qa'ida bombers from Kenya so they could be tried and convicted for the embassy bombings.

In 2000, I met with President Musharraf in Pakistan and negotiated the availability of a critical witness in one of our major terrorism prosecutions. I briefed him on the indictment against bin Ladin regarding the 1998 embassy bombings and asked for his assistance in capturing him in Afghanistan. FBI agents and a prosecutor from the United States Attorney's Office from the Southern District later returned to Pakistan to continue those efforts.

In 1996, I met with Presidents Nazarbayev and Karimov in Kazakhstan and Uzbekistan, of Kazakhstan and Uzbekistan, respectively, and discussed radical fundamentalist terrorism directed against the United States from Afghanistan and Iran. I asked for their help in fighting these threats to America.

I traveled extensively, as did scores of FBI men and women, throughout the Mideast, Central Asia, Africa, the Persian Gulf and South America with a very primary objective of strengthening our counterterrorism program so we could protect Americans at home.

Dozens of Special Agents went to places like the Triborder Area in South America, Southeast Asia, Africa, Greece, Georgia, Russia, and many other places to carry out our counterterrorism mission.

For example, these relationships have paid enormous benefits. When we were examining the forensic evidence from the USS *Cole* case, we discovered that the explosive used was probably manufactured in Russia. Because the FBI had been working in Russia since 1994, I was able to call the FSB Director and ask for assistance. His response was immediate. Russian explosive agents and experts provided the FBI with all the necessary forensic and expert information requested, helping the case immensely.

The 1996 Khobar bombing investigation demonstrates the FBI's successes and limitations in combating foreign-based terrorists who wage war against the United States. The FBI's 1996 Khobar bombing investigation is a prime example of the FBI's success in combating terrorism because of solid relationships with our foreign partners. It also points to the limitations in dealing with these acts strictly as criminal cases.

After that devastating terrorist attack on June 25, 1996 which killed 19 United States airmen and wounded hundreds more, the FBI was instructed to mount a full-scale criminal investigation. We immediately dispatched several hundred FBI personnel to Dhahran, Saudi Arabia, and, supported by our armed forces, established a crime scene, interviewed available witnesses, obtained evidence and set out leads and obtained a plan.

Working in close cooperation with the White House, State Department, the CIA, and the Department of Defense, I made a series

of trips to Saudi Arabia in order to further the FBI's investigation. Because of the FBI's prior contacts with the Saudi police service, the Mabaheth, and Interior Ministry had been carried on from offices as far away as Rome and Cairo, the FBI lacked any effective liaison or relationship with its counterpart agencies in Riyadh.

Fortunately, the FBI was able to forge an effective working relationship with the Saudi police and Interior Ministry. After several trips and meeting with the Saudi leadership, and particularly Prince Nayef, the Interior Minister, the FBI was granted permission to expand its presence and joint operational capability within the Kingdom.

I was particularly fortunate to gain the trust and cooperation of Prince Bandar bin Sultan, the Saudi Ambassador to the United States, who was critical in achieving the FBI's investigative objectives in the Khobar case. Due to Prince Bandar's forthcoming support and personal efforts, the FBI was able to establish an FBI office in Riyadh.

Our Arab-speaking Special Agent, who became the first FBI agent to be assigned to Saudi Arabia, quickly made critical liaison, and relationships of trust were established between the FBI and the Mabaheth. Evidence and access to important witnesses were obtained, and excellent investigative support was furnished to various teams of FBI agents who worked in Saudi Arabia to pursue the case. In one instance, Canadian authorities, acting on Saudi information, arrested a Khobar subject who was brought to the United States and thereafter sent by the Attorney General to Saudi Arabia for prosecution.

The cooperation the FBI received as a result of Prince Bandar's and Nayef's personal intervention and support was unprecedented and invaluable. From time to time, a roadblock or a legal obstacle would occur, which was expected given the marked differences between our legal and procedural systems. Despite these challenges, the problems were always solved by the personal intervention of Prince Bandar and his consistent support for the FBI.

The case almost faltered on the issue of the FBI's critical request for direct access to six Saudi nationals who were being detained in the Kingdom and who had been returned to Saudi Arabia from another country, who had key information which would later implicate senior Iranian Government officials as responsible for the planning, funding and execution of this attack. We needed direct access to these subjects because their admissions and testimony were critical to support our prosecution. Yet no FBI agent had ever been given such unprecedented access to detain the Saudi national, which access could potentially taint their prosecution under Islamic law. For the same reasons the FBI would have been very reluctant to allow Saudi police officers to come to the United States and interview a subject under like conditions. Moreover, by making these witnesses directly available to the FBI, the Saudis understood that they would be helping to provide evidence that senior officials of the Government of Iran were responsible for the Khobar attack.

Despite these extremely sensitive and complex issues, the Saudis put their own interests aside to aid the FBI and the United States. Supported by Prince Bandar, Prince Nayef, the police and Crown

Prince Abdullah decided to grant the FBI request to interview the detainees. Ambassador Wyche Fowler closely worked with me in this endeavor and we finally succeeded. Teams of FBI agents were then able to have access to these detainees and full debriefings were conducted in Saudi Arabia.

As a direct result of these and later interviews, the Department of Justice was able to return a criminal indictment in June 2001, charging 13 defendants with the murders of our 19 servicemen. The indictment was returned just days before the statute of limitations would have run on some of the criminal charges. This case could not have been made without the critical support and active assistance of Saudi Arabia and the State Department through Ambassador Fowler.

The direct evidence obtained strongly indicated that the 1996 bombings were sanctioned, funded and directed by senior officials of the Government of Iran. The Ministry of Intelligence and Security and the Iranian Revolutionary Guard Corps were shown to be culpable for carrying out the operation. The bombers were trained by Iranians in the Bekaa Valley. Unfortunately, the indicted subjects who were not in custody remained fugitives, some of whom are believed to be in Iran.

Khobar represented a national security threat far beyond the capability or authority of the FBI or Department of Justice to address. Neither the FBI Director nor the Attorney General could or should decide America's response to such a grave threat. While, on the one hand, Khobar demonstrated the capability of the FBI acting in cooperation with its foreign counterparts overseas to work successfully, under extremely complex conditions, to pursue criminal cases, it also demonstrated that an act of war against the United States, whether committed by a terrorist organization or by a foreign state, can receive only a limited response by the FBI making a criminal case.

Mr. Watson recounted a meeting that he and I had with you, Senator Shelby, and Senator Bob Kerrey. We came up to brief you on the Khobar attack and how the FBI case was proceeding. I remember very much as we discussed this, you and Senator Kerrey commended the FBI for working on this matter, but you also commented that the FBI was somewhat out of its depth combating an act of war much graver than merely a horrific crime. I never lost sight of that fact, and its truth is even more apparent after September 11.

The FBI always viewed these investigations as secondary to any national security action and severely limited in their overall impact on a faraway enemy such as al-Qa'ida. I always stress that the FBI investigations were completely secondary to the needs of our national security.

The National Commission on Terrorism made this point convincingly by using the pursuit of the Pan Am 103 case investigated by the FBI as an example of the more aggressive national strategy needed against this scale of terrorism. I quote from the Commission's finding:

"Law enforcement is designed to put individuals behind bars, but is not a particularly useful tool for addressing actions by states. The Pan Am 103 case demonstrates the advantages and limitations

of the law enforcement approach to achieve national security objectives. The effort to seek extradition of the two intelligence operatives implicated most directly in the bombing gained international support for economic sanctions that a more political approach may have failed to achieve. The sanctions and the resulting isolation of Libya may have contributed to the reduction of Libya's terrorist activities. On the other hand, prosecuting and punishing two low-level operatives for an object almost certainly conducted by Qadhafi is a hollow victory, particularly if the trial results in his implicit exoneration."

The Commission concluded that, "Iran remains the most active supporter of terrorism. The IRGC and MOIS have continued to be involved in the planning and execution of terrorist acts. They also provide funding, training, weapons, logistical resources, and guidance to a variety of terrorist groups, including Lebanese Hizbollah, Hamas, PIJ and PFLP–GC."

The Commission noted that "in October, 1999, President Clinton requested cooperation from Iran in the investigation of the Khobar bombing. Thus far, Iran has not responded. International pressure in the Pan Am 103 case ultimately succeeded in getting some degree of cooperation from Libya. The United States Government has not sought similar multilateral action in bringing pressure on Iran to cooperate in the Khobar Towers bombing investigation."

We must always recognize the limitations inherent in a law enforcement response. As we see at this very moment in history, others, to include Congress, must decide if our national will dictates a fuller response.

I'm going to skip the section on pages 89 to 102, I know without objection, with respect to our information technology issue, and say briefly there that we were far behind in our ability to acquire and have funded the information technology required by a competent law enforcement and counterintelligence/counterterrorism agency. There's a long history there. I've set it out for you. I take some responsibility for the delay.

The good news is that when I left the FBI, we were on track to the full funding of the Trilogy program, which this committee is well aware of and which will put us back in the race with respect to IT.

In addition to IT, other critical technology assistance is required for the FBI to continue an effective war against terrorism. In 1994, as a result of the FBI's own initiative, Congress passed the Communications Assistance to Law Enforcement Act, CALEA. This critical statute was vital to ensuring that law enforcement could maintain the technical ability to conduct court-authorized electronic surveillance. Against tremendous opposition, the FBI persuaded Congress that this selectively utilized technique was essential to working its most complex criminal and national security cases. Support from Chairman Leahy, Senator Hatch and many other Members was critical in this legislation.

The law simply allows the FBI to continue its court-controlled use of this capacity as the telecommunications world changes from an analog to a digital network. It has taken most of the last eight years to fund and implement CALEA, and faster progress needs to

be made. But CALEA simply permits the FBI to maintain court-approved access to digital communications and stored data.

Another technical challenge called "encryption" then and now threatens to make court-authorized interception orders a nullity. Robust and commercially-available encryption products are proliferating, and no legal means have been provided to law enforcement to deal with this problem, as was recently done by Parliament in the United Kingdom. Terrorists, drug traffickers and criminals have been able to exploit this huge vulnerability in the public safety matrix.

Many of you have heard me and others testify before you over the years about this problem. The International Association of Chiefs of Police, the 50 State attorneys general, the National Association of District Attorneys have all identified this problem as the most critical technology issue facing law enforcement. Many of you—Chairman Goss, who is not here right now, Representative Norm Dicks, Senator Kyl, Senator DeWine and Senator Feinstein particularly—have provided outstanding leadership and gone to great lengths to address this problem.

In 1998, HPSCI adopted a substitute bill to S. 909 which effectively addressed all of law enforcement, public safety and terrorism-related concerns regarding encryption products. Unfortunately, this needed counterterrorism assistance was not enacted. As we know now from Ramzi Yousef's encrypted computer files found in Manila, terrorists are exploiting this technology to defeat our most sophisticated methods to prevent their attacks.

I have long said, and repeat here today, that this unaddressed problem creates a huge vulnerability in our Nation's counterterrorism program. Neither the PATRIOT Act nor any likely-to-be enacted statute at this time even attempts to close this gap. Resolving this issue is critical for homeland security.

In 1995, Congress authorized the FBI to establish a Technical Support Center. The purpose of this facility was to provide Federal and local law enforcement with the technology tools to improve court-authorized telecommunication interceptions and signal access for investigative purposes. I was pleased to see that this critical center was fully funded subsequent to September 11.

Many other critical technology needs must be addressed both with legal authorization, such as the once-proposed Cyberspace Electronic Security Act bill, and significant new resources for counterterrorism, cyberterrorism, and dealing with weapons of mass destruction and proliferation. Unfortunately, the convergence of technology and globalization now enable an individual terrorist or a small group of terrorists operating from the other side of the world in a protected sanctuary—or operating in our backyard—enables them to threaten our Nation in devastating ways.

I think we need to acknowledge that the rules governing the FBI's counterterrorism efforts changed as a result of September 11. We must acknowledge that the rules are changing beginning with certain provisions of the USA PATRIOT Act. The Department of Justice and the intelligence agencies have been given new tools, as the statute is entitled, to combat a dangerous enemy who follows no rules. Some of these new authorities have been granted by the Congress with a sunset provision. Some asserted by the govern-

ment are being challenged in the courts, where they will ultimately be decided.

It must always be understood that prior to September 11 the FBI, as it always must, followed the rules as they were given to us by the Attorney General and the Congress. For example, FBI agents were not permitted, without special circumstances, to visit a suspect group's Web site or to attend its public meetings. Counterintelligence, domestic terrorism and informant guidelines promulgated years ago and updated with new restrictions curtailed our ability to collect information in national security cases.

Those guidelines are now being changed. "Primary purpose" requirements for FISA applications and information separation structures limited the sharing of criminal and intelligence information. Grand jury and Title III secrecy provisions severely restricted the dissemination of criminal terrorist information obtained during those processes.

I repeatedly testified before Congress that FBI agents were statutorily barred from obtaining portions of credit reports on national security subjects when used car dealers could order them and read them.

Before we interviewed detained foreign national al-Qa'ida subjects in East Africa in connection with the East African bombings, FBI agents duly gave them their Miranda rights.

When I left the FBI in June of 2001, we were being criticized in some quarters because a valuable new electronic tool necessary to read a terrorist's e-mail pursuant to a court order had the hypothetical potential to be abused—as any law enforcement tool could be.

Everyone understands why and how some of the rules changed after September 11. But it's important to understand that the rules were changed by changed circumstances and that those circumstances changed the standards and expectations of both the FBI and the CIA.

During my tenure as FBI Director, I was immensely proud of the cooperation and integration of FBI and CIA efforts to combat terrorism. Myself and recent DCIs, particularly George Tenet, have taken bold and unprecedented steps to work together and forge an effective FBI–CIA partnership to combat terrorism. Exchanging senior officers, standing up to the joint Usama bin Ladin/al-Qa'ida operations and intelligence center, fully coordinating our Legat and Station Chiefs, cross-training and many additional measures were taken to integrate our counterterrorism resources and capabilities. Our joint efforts in the East African bombings s is a template of how successful we were in working together.

Some of these efforts cannot be described in this session. This historical and successful integration does not mean that on every point of intersection a lapse did not occur. But to focus on those isolated instances while ignoring the huge successes of this top-down directed integration is misplaced. I personally credit George Tenet with making this happen and winning the trust and respect of the FBI in the process.

The best confirmation, by the way, of this fully integrated FBI–CIA counterterrorism effort is the fact that during my tenure no chairman or member of this committee ever raised with me or the

DCI, to my knowledge, the issue of our agencies being uncooperative or adverse to working together. Conversely, it was repeatedly pointed out to me by your committees that the FBI and CIA were working together in an exemplary manner.

I end with some recommendations:

One, provide legal authority and significant new funding enabling the FBI to manage in encryption technology;

Two, significantly increase the number of FBI Special Agents and support positions with sufficient compensation required to recruit and retain the best men and women to combat terrorism;

Three, significantly increase the FBI's technical support program and facilitate the FBI's access to emerging technologies and research and development by the private sector;

Four, significantly increase the number and staffing and FBI's Legat officers overseas;

Five, exempt the FBI from the compensation restrictions of Title V;

Six, change the FBI's procurement procedures to facilitate the efficient design and acquisition of equipment and technology;

Seven, provide new funding for the FBI's international training programs and put the FBI in charge of all international law enforcement training;

Eight, fund whatever it takes to achieve interoperability between all the agencies engaged in the war against terrorism;

Nine, restructure the budget to give more flexibility to the DCI, Attorney General and the FBI Director to better allocate program funding and resources as missions evolve and new threats emerge;

Ten, consider establishing a domestic public safety office in the executive with responsibility for coordinating and supporting national law enforcement issues; and

Finally, enhance the legal, technological and funding resources of the FBI rather than consider creating an intelligence agency to share its domestic, public safety responsibilities.

In conclusion, the FBI and CIA working together have accomplished much in fighting terrorism at home and abroad, but it is a constant and continuing battle. These agencies should remain the primary counterterrorism agencies for this mission.

The DCI's authority for coordinating and implementing government-wide efforts in this regard should be expanded. The war against terrorism must be waged relentlessly. It will require that significantly more resources be allocated to the FBI and CIA. These fine agencies and the brave men and women who fight this war cannot defeat some forms of terrorism without total government intervention no matter how great and heroic their efforts. Al-Qa'ida-type organizations, state sponsors of terrorism like Iran and the threats they pose to America, are beyond the competence of the FBI and the CIA to address. America must maintain the will in some cases to use its political, military and economic power in response when actions of war are threatened or committed against our Nation by terrorists or their state sponsors.

Finally, however treacherous the enemy, the FBI must fight this war as a law enforcement agency of the Department of Justice governed by the rule of law and the Constitution. The rules, statutes and guidelines which establish the legal authorities of the FBI may

change—as they did significantly after September 11—as long as those changes are clearly defined and understood.

The FBI's adherence to the Constitution and the rule of law must not change. We do not have to sacrifice our freedoms to protect them.

Thank you.

Chairman GRAHAM. Thank you, Mr. Freeh.

Ms. White.

[The prepared statement of Ms. White follows:]

STATEMENT OF

MARY JO WHITE

FORMER UNITED STATES ATTORNEY
FOR THE SOUTHERN DISTRICT OF NEW YORK

before the

Joint Intelligence Committees

October 8, 2002

October 8, 2002

STATEMENT OF MARY JO WHITE

Before the Senate Select Committee
on Intelligence and House Permanent
Select Committee on Intelligence
Joint Inquiry into the September 11th
Terrorist Attacks

Mr. Chairmen, members of the Committees, thank you for inviting me to testify before you in this very important joint inquiry. It goes without saying that the terrorist attacks of September 11th profoundly affected and changed each one of us and our nation forever. But the most grievously impacted are obviously the loved ones of those who were so wantonly murdered without warning that day. It is to them that we most owe whatever answers there are to be found for how it happened and the assurance that we, as a government, have done, and will continue to do, everything in our power to prevent such human devastation from ever happening again.

Recognizing the comparative narrowness of the perspective and knowledge that I have on this very complex subject, I am honored to share it for whatever use it may be to your inquiry. This written statement, which is submitted for the record, summarizes that perspective and knowledge from my experience as the United States Attorney for the Southern District of

New York from June 1, 1993 until January 7, 2002. In the course of my statement, I attempt to address the specific questions in your letter of September 17, 2002, inviting my testimony. I would also be pleased to answer any additional questions the Committees may have of me today, or in the future as your work goes forward.*

A. International Terrorism Investigations and Prosecutions in the United States Attorney's Office for the Southern District of New York ("SDNY USAO").

From the beginning of my tenure as United States Attorney in 1993 to its last day in 2002, I, together with a number of extraordinarily dedicated and talented Assistant United States Attorneys ("AUSAs"), agents and detectives from the FBI-NYPD Joint Terrorist Task Force (the "JTTF"), was actively involved in the investigation and prosecution of international terrorists and terrorist organizations who were plotting to attack, or had actually attacked, Americans and American interests, both in the United

* I have also included as an appendix to this statement copies of three of the talks that I have given on international terrorism since September 11th; they summarize some additional thoughts on what we have learned about the nature of the threat from international terrorists and what we must do in the future to address that threat, as well as my views on military tribunals.

States and abroad.* No work in our office of over 200 very busy and productive AUSAs received a higher priority.

The international terrorism work of the SDNY USAO began with the investigation and prosecution of those responsible for the bombing of the World Trade Center ("WTC") on February26, 1993, in which six people were killed and over 1,000 were injured. It included the investigation and eventual indictment of Usama bin Laden ("UBL"), the leader of the al Qaeda terrorist organization, first in June 1998 for conspiracy, under seal, before he or al Qaeda had massively attacked anyone. (A copy of the June 1998 indictment of bin Laden is at Tab A.) Bin Laden and 22 other defendants were subsequently indicted in November 1998, for their role in the

---

* In May 1980, the New York FBI Office and the New York City Police Department formed the JTTF to investigate a rash of terrorist bombings then occurring in New York City. The theory of the JTTF was that interagency cooperation is essential to any effective counterterrorism strategy. In addition to the FBI and NYPD, the New York JTTF includes the ATF, Secret Service, INS, FAA, New York State Police, U.S. Department of State, U.S. Customs, the New York and New Jersey Port Authority Police, the U.S. Marshals, the Amtrak Police, the Suffolk County Police Department, the Naval Criminal Investigative Service, and the Metropolitan Transit Authority Police. The New York JTTF became the template for other JTTFs formed across the county, both before and after September 11th.

bombings of the U.S. embassies in East Africa on August7, 1998, in which 224 innocent people, including 12 Americans lost their lives. In addition to the prosecution of those who bombed the World Trade Center in 1993 and those who bombed our embassies in Nairobi, Kenya and Dar es Salaam, Tanzania in 1998, the SDNY USAO also successfully prosecuted approximately twenty additional terrorist defendants for their roles in three other major terrorist plots, which were fortunately thwarted by law enforcement: the 1993 Day of Terror Plot to blow up government buildings and other structures in New York City; the 1994 Manila Air Plot to blow up a dozen U.S. jumbo jets flying back to America from the Far East; and the December 1999 Millennium Plot of Ahmed Ressam, an Algerian terrorist trained in al Qaeda camps in Afghanistan, to detonate a bomb at the Los Angeles International Airport.*

In all, the SDNY USAO charged and convicted over 30 defendants for international terrorism; there were no acquittals. All of the defendants are

* In 2001, the Seattle USAO successfully prosecuted Ressam and the SDNY USAO successfully prosecuted two defendants who from New York provided material assistance to Ressam's plot in the form of money, credit cards, and phony identification papers.

serving life or very lengthy prison sentences, without the possibility of parole. There are, however, fugitives still at large in several of the cases, including bin Laden himself who, as of September 11th, had been under indictment for over three years and on the FBI's Ten Most Wanted List for over two years. Fifteen of the 22 terrorists on The Most Wanted Terrorist List, announced by President Bush on October 10, 2001, are fugitives in the SDNY cases -- thirteen from the Embassy bombings case; one from the 1993 bombing of the WTC (Abdul Rahman Yasin, who fled New York on the day of the 1993 WTC bombing and who was recently interviewed on "60 Minutes," in a broadcast televised from Iraq); and one defendant from the Manila Air Plot (Khalid Sheik Mohammed, who has been widely reported in the media to be one of the major planners of the September 11th attacks).

B. When the Threat of International Terrorism Was Regarded As a Threat to and in America and the Importance of the Day of Terror Plot

Certainly, by the time our embassies in East Africa were bombed in 1998, we as a government knew a great deal about the threat posed by bin Laden and al Qaeda to America and, at least by the time the Embassy bombings indictment was filed in 1998 , much of that knowledge was a

matter of public record. But the high risk that international terrorist posed to America, both in America and abroad, was known and appreciated as a significant threat from at least 1993.

The bombing of the World Trade Center on February26, 1993 itself, of course, represented a dramatic incident of international terrorism hat Ramzi Yousef, one of its masterminds, had brought from abroad to America. But it was the follow-on terrorist plot in 1993 (the Day of Terror Plot) to blow up in a single day the Lincoln and Holland Tunnels connecting New York and New Jersey, the George Washington Bridge, the U.N., and the New York FBI office in lower Manhattan that led at least those of us in the SDNY USAO and FBI to conclude that international terrorism was a long-term, highly dangerous risk to the safety and national security of theUnited States. The FBI and other public officials testified to this risk and spoke about it publicly to citizens groups. Prior to September11th, I personally gave several talks discussing specifically the point that international terrorism had come fromabroad to America and posed a significant continuing threat to America, both at home and abroad. (A copy of one such talk to the Middle East Forum on September27, 2000 is attached at Tab B.)

The Day of Terror Plot, headed by the blind cleric and leaderof the G'amaat terrorist organization, Sheik Omar Abdel Rahman, was fortunately foiled by the New York FBI and the JTTF because they had been able to infiltrate the terrorist cell operating in the New York-New Jersey metropolitan area with an informant posing as an explosives expert. As a result, the plot could be – and was – carefully monitored and stopped before it could come to fruition. The evidence necessary for the successful prosecution of Sheik Rahman and eleven of his followers was also obtained. It was, in short, a very successful prevention and prosecution effort by the New York FBI and the JTTF.

The Day of Terror Plot case thus illustrates one point I want to make today and that is that, at least from our perspective, we viewed the terrorist investigations and prosecutions we did from 1993-2002 as a prevention tool. Everyone's goal was to thwart plots before they occurred and to neutralize dangerous terrorists so that they could not attack in the future. In that effort, we worked very closely with the FBI and, especially later, the CIA and other intelligence agencies, to ensure that the first priorities were always prevention and national security. When criminal investigations and

prosecutions could aid the overall national security effort, we willingly and aggressively offered our help.

From my vantage point, the counterterroristm strategy of our country in the 1990s was not, as I have read in the media, criminal prosecutions. Rather, criminal prosecutions were one tool in our couterterrorism efforts, a tool that certainly neutralized for life a number of very dangerous international terrorists, including Ramzi Yousef, a mastermind of the 1993 WTC bombing and the architect of the Manila Air Plot, and Sheik Omar Abdel Rahman, the leader of the Day of Terror Plot and head of the G'amaat terrorist organization that later joined forces with al Qaeda. It was also, of course, our hope that the indictment of UBL and the leadership of al Qaeda in 1998 would result in the apprehension and neutralizingof these and other terrorists who posed– and still pose – very grave threats to the safety of America and the world. But none of us considered prosecutions to be the country's counterterrorism strategy, or even a major part of it.

In addition to cementing our view that international terrorism posed a significant threat to us here at home, the Day of Terror Plot is also instructive for a number of other reasons. First, it showed the foothold that

international terrorists had or were gaining in the United States – all of the defendants in the case were residing in New York and New Jersey; some were here legally, some illegally.* The Sheik was preaching his anti-American rhetoric in mosques in Brooklyn, New York and Jersey City, New Jersey.

Second, and even more importantly, the Day of Terror Plot illustrates the importance of the infiltration of terrorist cells by human sources and informants. Such infiltration is, in my view, one of the most effective means of preventing terrorist attacks. It is not easy to do. There are significant language, cultural and expertise barriers that must be overcome. There is also always the risk that the informant can be or become a double agent who may facilitate rather than prevent an attack. Nevertheless, in my view, whatever can be done to enhance the FBI's and the Intelligence Community's ability to develop human sources and operatives capable of

* There is no doubt, in my mind, that it is a critical matter of national security that our immigration policies and procedures be dramatically enhanced. A number of the terrorist defendants in the SDNY cases, including Ramzi Yousef, entered the country illegally or remained in the country illegally, only to surface when they participated in a terrorist attack in the United States.

infiltrating terrorist cells should be done, both in the United States and around the world.

At the conclusion of the trial of the Day of Terror Plot in 1995, I made the decision to form an international terrorism unit in the SDNY USAO and to staff it initially with those half a dozen AUSAs who had been involved in the investigations and prosecutions of the 1993 WTC bombing,the Day of Terror Plot, and the Manila Air Plot.* I personally supervised the unit. I made the decision to establish a permanent terrorism unit because we had concluded that the risk of future terrorist attacks and plots was high and long-term and because, as a result of the knowledge we and the New York FBI and JTTF had gained as a result of the two backto-back 1993 international terrorism cases, we had, of necessity, amassed a great deal of intelligence about various terrorists and terrorist networks hat we did not want to lose as we went forward. We wanted to pursue all leads of other terrorist conspiracy and attacks. So, unlike with other kinds of prosecutions,

* The SDNY USAO Terrorism Unit was, to my knowledge, the only terrorism unit in any USAO prior to September 11th.

we did not close up shop after the Day of Terror Plot after the defendantss were convicted and went to jail.

We did not wait for the next attack. We, together with the FBI and JTTF, actively continued to investigate other possible terrorist crimes and conspiracies, to try to learn more, to follow any lead that suggested itself from the facts we did know. Even in 1995, there was a mass of names and snippets of information, certainly not fully understood, but still information bits to be pursued and to learn more about if we could. We learned more each day, and we are continuing to learn moreeach day. The work of these AUSAs, the FBI and the other agents and police officers on the JTTF, together with others in our government including the Intelligence Community, eventually culminated in the indictment of bin Laden and the al Qaeda leadership, and the conviction of over thirty dangerous terrorists. Equally important, it led to a growing body of information on international terrorists, their organizations and operations, including from a growing number of cooperating defendants who provided valuable intelligence information.

In sum, in our view, there was no dichotomy between prevention and prosecutions. Prosecutions were and are part of the prevention effort, as well as a means of bringing terrorists to justice for their terrorist crimes, whether or not the crimes have culminated in an actual attack, as they did in the 1993 WTC bombing and the 1998 East African Embassy bombings, or were stopped at the stage of a conspiracy, or plot that had not ripened into an actual attack, as was the case in the Day of Terror Plot, the Manila Air Plot, the indictment of UBL in June 1998 for conspiracy, and the Millennium Plot of Ahmed Ressam. The ultimate, overarching objective of all involved, including the U.S. Attorney's Office and the FBI, was to obtainthe information and evidence of a planned attack or plot and to stop it before it occurred. While it is the reality that not every terrorist attack can be prevented, our objective and priority must always be a perfect prevention success rate. We must do whatever is lawful in our effort to achieve that.

C. The Role and Effectiveness of Criminal Prosecutions

As the SDNY cases demonstrate, criminal prosecutions of terrorist defendants have been and can be effective tools to deal with terrorists who commit federal crimes and as to whom there is sufficient, available evidence

to prove such defendants' guilt beyond a reasonable doubt under the rules governing criminal trials in the American criminal justice system.* Prosecutions can also lead – and did lead – to cooperating defendants who provided invaluable intelligence on the terrorism threat, as well as trial testimony. These prosecutions also neutralized for life or many years a number of very dangerous terrorists who would have otherwise continued to commit further terrorist attacks: some bombs were thus undoubtedly not built and detonated; some planes were not blown up; and some people were not assassinated. That is obviously good.

But criminal prosecutions are plainly not a sufficient response to international terrorism. For that, we plainly need more comprehensive measures and, most especially a strong and continuing military response. This is my view today and was my view prior to September 11th.

---

* Often in international terrorism cases, there is evidence of a terrorist defendant's guilt which cannot be used by prosecutors because its public disclosure may compromise intelligence sources or other national security interests. As we understood at the outset of the terrorism prosecutions, the prosecutors must always be prepared to defer to such overriding interests, and we did.

There are a number of obvious limitations on the abilityof our criminal justice system to effectively and broadly combat international terrorism. These include the following:

- Criminal prosecutions of international terrorists have limited deterrent effect. When thousands of international terrorists all over the world are willing, indeed anxious, to die in service of their cause, we cannot expect prosecutions to effect significant deterrence. Each of the SDNY cases I have mentioned in this statement followed the one before it, culminating most recently in the attacks of September 11th. Prosecuting and convicting Ramzi Yousef for the 1993 WTC bombing and the Manila Air Plot did not deter other would-be terrorists from bombing our embassies in East Africa in 1998 or from hijacking and flying those planes into the WTC and the Pentagon on September 11th

- Criminal prosecutions create unique security issues for witnesses, juries, prosecutors, defense attorneys, judges and the Bureau of Prisons. While those risks can be managed in a limited number of cases, it is neither realistic nor wise to assume such risks routinely. International terrorists are not routine criminals.

- Much of the evidence necessary to prosecute international terrorists increasingly comes from abroad and is often obtained by foreign officials under very different systems and rules. This creates an array of difficult issues, including novel questions of law, and uncertainty about the admissibility and the continued availability of important witnesses and evidence.

These issues were especially pronounced in the Manila Air Plot and East Africa Embassy bombing cases.*

- The criminal discovery rules governing criminal trials, coupled with the extensive amount of classified and otherwise sensitive information that relates to international terrorism cases, make successfully prosecuting terrorist defendants, while at the same time safeguarding intelligence sources and methods, extremely difficult. Although I believe we successfully achieved that balance in all of the SDNY cases, it is an ever-present and very difficult issue and risk.

D. The Sharing and Dissemination of Information Related to the Threat of International Terrorism

I understand that one of the Committees' concerns is whether, prior to September 11th, the information about international terrorism gathered by the various parts of our law enforcement and intelligence communities was shared and disseminated sufficiently. This is one of those areas where I

---

* At times, critical witnesses or evidence the prosecutors had assumed and been promised were available from foreign sources, proved not to be so when the time of trial arrived. In this regard, it is important to point out the significance of the personal involvement and work of FBI Director Louis Freeh to the successful prosecutions of international terrorists in the SDNY, as well as other international terrorism cases. Director Freeh established the FBI as a global presence and formed the necessary cooperative relationships with his counterparts around the world to make possible successful investigations, prosecutions and thwarting of terrorist attacks. He also personally and repeatedly dealt with heads of governments and agencies to secure critical evidence, testimony and cooperation.

must defer to others who have the complete picture. While we certainly had concerns about this, my general impression was that the information and evidence developed in at least the terrorism investigations and prosecutions in the SDNY was generally shared by the FBI with the Intelligence Community and other parts of our government, as well as with local and state authorities. Much of the information was, in fact, developed by the Intelligence Community and local and state agencies worked directly on the JTTF which worked each of the SDNY cases.

I cannot speak to what information the IntelligenceCommunity may have had that was not shared with the FBI or law enforcement generally, but I can say that the relationship was a very positive and cooperative one. The CIA, in particular, was of invaluable assistance in the SDNY cases and investigations. I can also say from my personal experience as a prosecutor and U.S. Attorney for many years that, under the leadership of FBI Director Louis Freeh and DIA George Tenet, the working relationship and cooperation between the FBI and the Intelligence Community at their highest levels was excellent and saw a seachange of improvement in the 1990s in the ranks of the agencies as well. Nowhere was this cooperation

more apparent and productive than in the investigation of the terrorist threat posed by al Qaeda and bin Laden.

It is also important to recall that a great deal of the information and evidence developed in the SDNY investigations and prosecutions had become public through indictments and public trials, long before September 11th. Perhaps one of the best summaries of what was publicly known about the threat bin Laden and the al Qaeda terrorist organization posed to America prior to September 11th is in the indictment returned and filed in the SDNY in 1998 following the August7, 1998 bombing of our embassies in Nairobi, Kenya and Dar es Salaam, Tanzania. (The indictment is at Tab C of this statement.) The information in the indictment was later amplified publicly at the trial of four of UBL's followers who were convicted in the SDNY in May 2001 for their roles in the bombings. The Embassy bombings indictment sets forth, among other facts, the following:

- Bin Laden and al Qaeda's top leadership are named as defendants, including Aymad Al Zawahiri, the head of Egyptian Islamic Jihad, Muhammed Atef, the military commander of al Qaeda, and Mamdouh Mahmud Abdullah, al Qaeda's financial director.
- The command and control structure of al Qaeda is detailed.

- Al Qaeda's wealth and businesses used to raise money for terrorist operations are detailed.
- The worldwide reach of al Qaeda, including its presence within the United States is detailed.
- Bin Laden's alliance with the National Islamic Front in Sudan and with representatives of the Iranian government and Hizballah for the purpose of working together against their common enemies in the West, including the United States, is detailed.
- Bin Laden's efforts to acquire the components for nuclear and chemical weapons are set forth.
- Al Qaeda's role in training those in Somalia who killed eighteen American soldiers in October 1993 as they served as part of the U.N.'s Operation Restore Hope is set forth.
- The details of the simultaneous bombings of our American embassies in Kenya and Tanzania on April 7, 1998 are set forth in 224 separate murder counts for those killed, including 12 Americans.
- Efforts to recruit American citizens as workers and members of al Qaeda are described.
- The al Qaeda conspiracy to kill Americans dating from at least 1991 is detailed.
- Bin Laden's fatwas directing Muslims to kill all Americans, including civilians, wherever in the world they can be found, are recited.

This may be the right juncture to talk about another point relating to the dissemination of information. The issue is what limitations, prior to its

amendment in the USA Patriot Act, did the grand jury secrecy rules, embodied in Rule 6(e) of the Federal Rules of Criminal Procedure, impose on the sharing of information between the law enforcement and the Intelligence Community. My view is that Rule 6(e) was not a significant barrier to the sharing of information developed in the SDNY investigations and prosecutions.

Rule 6(e) of the Federal Rules of Criminal Procedure, prior to its amendment in the USA Patriot Act after September 11th, did not make provision for providing grand jury informationto intelligence agencies for purposes of safeguarding the national security, either with or without a court order. Thus, if information was obtained through the grand jury by prosecutors, or criminal division agents of the FBI working with prosecutors and the grand jury, Rule 6(e) could operate to prevent the sharing of the information with, for example, the CIA.

It has been said by some, I gather, that, as a result of Rule 6(e) and grand jury secrecy, there was a "treasure trove" of grand jury informationin the files of the prosecutors in the SDNY and the FBI that could not be and was not shared with the Intelligence Community. Although plainly Rule

6(e), prior to its amendment, posed the risk of insulating relevant information at least until trial, I donot believe that it did so in the SDNY investigations and prosecutions. (I have confirmed my understanding on this point with the Assistants in my office who were in charge of the investigations.)*

Grand jury secrecy rules do not appear to have impeded he sharing of information in the SDNY investigations and prosecutions for several reasons. First, the vast majority of information obtained was not obtained through the grand jury, but by non-grand jury means of investigation to which grand jury secrecy rules do not apply. Second, if any relevant information was obtained through the grand jury to which Rule 6(e) might apply, we were generally able to obtain it through alternative means as well so that it could be shared. Third, quickly over time, the information we and the FBI obtained in our investigations became a matter of public record through publicly filed indictments and other court documents, as well as

* The SDNY USAO would not itself generally pass information tothe intelligence or national security communities. By policy and protocol, it would be conveyed by either the FBI or DOJ.

public trials with detailed written transcripts and publicly filed exhibits. (I earlier cited the East Africa Embassy bombing indictment and trial as one example of the amount and range of information publicly available on the threat of international terrorism and on bin Laden and al Qaeda, in particular.)

That the grand jury secrecy rules did not impede the sharing of information in the SDNY cases is not to say that the grand jury secrecy rules might not have prohibited the sharing of information with the intelligence and national security communities. They could well have, which is why I advocated, when asked by FBI Director Robert Mueller and representatives of the Department of Justice shortly after September 11th for recommended legislative changes, that Rule 6(e) be amended to permit the sharing of national security-related information with the Intelligence Community.* One final point on this: our constant mindset was to try to maximize the sharing of information real-time so that it could hopefully be used by others

* This was a part of my very strong recommendation to "get the walls down" between the intelligence and law enforcement parts of our government dealing with terrorism.

to gain further information and, most importantly, to be used to possibly detect terrorist plots and to safeguard against any threats posed.

This leads me to another point about information sharing, but in the other direction. If I were to single out one significant concern that I had about our counterterrorism efforts prior to September 11th (dating from at least 1995), it was that I feared we could be hampered in our efforts to detect and prevent terrorist attacks because of the barriers between the intelligence side and law enforcement side of our government. Some of these bariers were (and perhaps still are) statutory; some were (and perhaps still are) cultural; some were (and still are) court-imposed; some were (and may still be) voluntarily imposed by the agencies by way of guidelines to assure compliance with all legal requirements and to make an adequate record of such compliance.

Our Intelligence Community is charged with gathering foreign intelligence to protect the national security. The FBI has a foreign counter intelligence function and law enforcement or criminal function. The functions are separately staffed. International terrorism, however, cuts across both of these functions; it does not fit as neatly into one category or

the other as espionage may have during the Cold War. Much of the information gathered in by the Intelligence Community is most often also evidence of a possible criminal conspiracy or other crime. Much of the information gathered by law enforcement as evidence of a terrorist-related plot is also most often foreign intelligence information relevant to the national security. And yet, at least as things were done in the 1990s through September 11th, that evidence, if gathered on the intelligence side, could not be shared with prosecutors unless and until a decision was made in the Justice Department, that it was appropriate to pass that information "over the wall" to prosecutors, either because it showed that a crime had been committed that needed to be dealt with by an arrest or further overt investigation, or because evidence of such crime was relevant to an ongoing criminal investigation. Because of this structure and these requirements, I do not know even today what evidence and information that might have been relevant to our international terrorism investigations were never passed over the wall.

To make a decision to pass information over the wall requires, in the first instance, a recognition of what that information is and what its

significance is. In the area of international terrorism, this is a very difficult task, made more difficult by a combination of language and cultural barriers, coded conversations, literally tens of thousands of names of subjects that are confusing and look alike, and an unimaginably complex mass of snippets of information that understandably may mean little to the people charged with reviewing and analyzing the information and deciding whether to recommend that it be "passed over the wall."

A prosecutor or criminal agent who has for years been investigating particular terrorist groups or cells and who has thus amassed a tremendous body of knowledge and familiarity with the relevant names and events might well recognize as significant what seems to other conscientious and generally knowledgeable agents or lawyers as essentially meaningless. What can happen, and I fear may have happened, is that the two halves of the jello box are never put together so that the next investigative step that could eventually lead, when combined with other information or steps, to the detection and prevention of a planned terrorist atack does not occur.

We must, in my view, do everything conceivably possible, to eliminate all walls and barriers that impede our ability to effectively counter

the terrorism threat. If policy and culture have to change to do that, they must change. If the law must be changed to do that, I would change the law. Indeed, I believe the Justice Department and Congress thought that the law had been changed to help address this problem by the USA Patriot Act. A recent decision by the Foreign Intelligence Surveillance Act ("FISA") court (now on appeal), however, suggests otherwise. In re All Matters Submitted to the Foreign Intelligence Surveillance Court, filed May 17, 2002.

That court decision also alludes to certain enhancements to the "wall" that the FISA court imposed prior to September 11th, effectively making the court the wall in certain international terrorism investigations. The walls that so concerned us throughout my tenure as United States Attorney thus were built higher prior to September 11th. While we were not made privy to the full rationale for the decision and would not condone any misrepresentations to any court or any abuse of the FISA authority, raising the walls did concern us greatly from a public safety point of view. We voiced those concerns with officials in the Department of Justice prior to September 11th. We do not know what, if any, relevant information was kept behind the wall.

Again, others who were and are behind no walls and fully privy to all of the facts will have to give you the complete picture. But from my vantage point, it appeared to me that the bifurcation of intelligence gathering and law enforcement, together with the requirements of FISA (prior to its amendment) requiring, in the view of some, that "the primary purpose" of every FISA search had to be for national security purposes impeded the FBI in its foreign counter intelligence function. Part of the problem appeared to stem from how conservative the Justice Department was in seeking FISA search authority in terrorism investigations when there were also ongoing criminal investigations and prosecutions on the same general subject because of the fear that a court would decide, in some later prosecution, that the FISA authority had been abused and used by the FBI to circumvent the generally stricter requirements of Title III to obtain a court-authorized wiretap for a criminal investigation.

The conservatism was, to a point, understandable. Some courts had decided that the FISA authority could only be used if "the primary purpose" of the search was to safeguard national security. When there were parallel ongoing criminal and intelligence investigations, there was a greater chance

that a court would find that the FISA authority had been inappropriately used. And plainly, no one wanted to risk losing the FISA authority, which is so vital to safeguarding the national security. But, in my view, the Department may have been too conservative in seeking approval for FISA searches out of excessive concern for the litigation risk should there be a criminal prosecution in which the FISA search was challenged.

This same conservatism stemming from the same concerns, I believe, may have spilled over to what was allowed to be passed "over the wall" to prosecutors and criminal agents, thus creating my nightmare of the two halves of the jello box never being put together. We cannot, as we go forward, risk these gaps in our intelligence gathering, sharing or analysis.

The single most important recommendation I would make to the Committees would be to address the full range of issues presented by the bifurcation of the intelligence and law enforcement communities and functions, as they operate in international terrorism investigations, including the permissible use of FISA and the dissemination and use of the product of FISA searches and surveillances.

E. Some Specific Recommendations.

The specific recommendations contained in my statement are:

1. Address and eliminate wherever possible the bifurcation of the intelligence and law enforcement functions in international terrorism investigations.

2. Make the necessary legislative and policy changes to FISA to address the bifurcation issue. Deal with privacy and abuse concerns through enhanced accountability.

3. Set up a mechanism to ensure that all relevant intelligence about international terrorism is, in fact, being fully shared, analyzed and disseminated real-time.

4. Gain control over our borders through a dramatic enhancement of the INS and its procedures.

5. Enhance the ability of the FBI and the Intelligence Community to develop and use human sources to infiltrate terrorist organizations.

Conclusion

Thank you for giving me this opportunity to share my perspective and concerns with the Committees. I am very grateful for your efforts. Your work is critical to the future of our nation and the world.

Mary Jo White

APPENDIX

1. "Prosecuting Terrorism in the Criminal Justice System," address given by Mary Jo White on October 4, 2002 at the University if Illinois at Urbana-Champaign, Conference on Rethinking Terrorism and Counterterrorism Since 9/11.

2. "Terrorism: A Law Enforcement Perspective," address by Mary Jo White on June 14, 2002 to the Philadelphia Police Department at a Counter-Terrorism Seminar.

3. "The Criminal Justice Response to Terrorism," address given by Mary Jo White on March 27, 2002 at the Yale Law School.

Tab A

SDNY indictment of Usama bin Laden to destroy U.S. defense facilities, filed under seal, June 1998.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

USAMA BIN LADEN,
a/k/a "Usamah Bin-Muhammad Bin-Laden,"
a/k/a "Shaykh Usamah Bin-Laden,"
a/k/a "Mujahid Shaykh,"
a/k/a "Abu Abdallah,"
a/k/a "Qa Qa,"

Defendant.

INDICTMENT

98 Cr.

COUNT ONE

Conspiracy to Attack Defense Utilities of the United States

The Grand Jury charges:

Background: Al Qaeda

1. At all relevant times from in or about 1989 until the date of the filing of this Indictment, an international terrorist group existed which was dedicated to opposing non-Islamic governments with force and violence. This organization grew out of the "mekhtab al khidemat" (the "Services Office") organization which had maintained (and continues to maintain) offices in various parts of the world, including Afghanistan, Pakistan (particularly in Peshawar) and the United States, particularly at the Alkifah Refugee Center in Brooklyn. From in or about 1989 until the present, the group called itself "Al Qaeda" ("the Base"). From 1989 until in or about 1991, the group was headquartered in Afghanistan and Peshawar, Pakistan. In or about 1992, the leadership of Al Qaeda, including its "emir" (or prince) USAMA BIN LADEN, the defendant, and its military command relocated to the

Sudan. From in or about 1991 until the present, the group also called itself the "Islamic Army." The international terrorist group (hereafter referred to as "Al Qaeda") was headquartered in the Sudan from approximately 1992 until approximately 1996 but still maintained offices in various parts of the world. In 1996, USAMA BIN LADEN and Al Qaeda relocated to Afghanistan. At all relevant times, Al Qaeda was led by its "emir," USAMA BIN LADEN. Members of Al Qaeda pledged an oath of allegiance to USAMA BIN LADEN and Al Qaeda.

2. Al Qaeda opposed the United States for several reasons. First, the United States was regarded as "infidel" because it was not governed in a manner consistent with the group's extremist interpretation of Islam. Second, the United States was viewed as providing essential support for other "infidel" governments and institutions, particularly the governments of Saudi Arabia and Egypt, the nation of Israel and the United Nations, which were regarded as enemies of the group. Third, Al Qaeda opposed the involvement of the United States armed forces in the Gulf War in 1991 and in Operation Restore Hope in Somalia in 1992 and 1993. In particular, Al Qaeda opposed the continued presence of American military forces in Saudi Arabia (and elsewhere on the Saudi Arabian peninsula) following the Gulf War. Fourth, Al Qaeda opposed the United States Government because of the arrest, conviction and imprisonment of persons belonging to Al Qaeda or its affiliated terrorist groups, including Sheik Omar Abdel Rahman.

3. Al Qaeda has functioned both on its own and through some of the terrorist organizations that have operated under its

umbrella, including: the Islamic Group (also known as "al Gamaa Islamia" or simply "Gamaa't"), led by co-conspirator Sheik Omar Abdel Rahman; the al Jihad group based in Egypt; the "Talah e Fatah" ("Vanguards of Conquest") faction of al Jihad, which was also based in Egypt, which faction was led by co-conspirator Ayman al Zawahiri ("al Jihad"); Palestinian Islamic Jihad; and a number of jihad groups in other countries, including Egypt, the Sudan, Saudi Arabia, Yemen, Somalia, Eritrea, Kenya, Pakistan, Bosnia, Croatia, Algeria, Tunisia, Lebanon, the Philippines, Tajikistan, Chechnya, Bangladesh, Kashmir and Azerbaijan. In February 1998, Al Qaeda joined forces with Gamaa't, Al Jihad, the Jihad Movement in Bangladesh and the "Jamaat ul Ulema e Pakistan" to issue a fatwah (an Islamic religious ruling) declaring war against American civilians worldwide under the banner of the "International Islamic Front for Jihad on the Jews and Crusaders."

4. Al Qaeda also forged alliances with the National Islamic Front in the Sudan and with the government of Iran and its associated terrorist group Hezballah for the purpose of working together against their perceived common enemies in the West, particularly the United States. In addition, al Qaeda reached an understanding with the government of Iraq that al Qaeda would not work against that government and that on particular projects, specifically including weapons development, al Qaeda would work cooperatively with the Government of Iraq.

5. Al Qaeda had a command and control structure which included a majlis al shura (or consultation council) which discussed and approved major undertakings, including terrorist

operations.

6. Al Qaeda also conducted internal investigations of its members and their associates in an effort to detect informants and killed those suspected of collaborating with enemies of Al Qaeda.

7. From at least 1991 until the date of the filing of this Indictment, in the Sudan, Afghanistan and elsewhere out of the jurisdiction of any particular state or district, USAMA BIN LADEN, a/k/a "Usamah Bin-Muhammad Bin-Laden," a/k/a "Shaykh Usamah Bin-Laden," a/k/a "Mujahid Shaykh," a/k/a "Abu Abdallah," a/k/a "Qa Qa," the defendant, and a co-conspirator not named as a defendant herein (hereafter "Co-conspirator") who was first brought to and arrested in the Southern District of New York, and others known and unknown to the grand jury, unlawfully, willfully and knowingly combined, conspired, confederated and agreed together and with each other to injure and destroy, and attempt to injure and destroy, national-defense material, national-defense premises and national-defense utilities of the United States with the intent to injure, interfere with and obstruct the national defense of the United States.

Overt Acts

8. In furtherance of the said conspiracy, and to effect the illegal object thereof, the following overt acts, among others, were committed:

a. At various times from at least as early as 1991 until at least in or about February 1998, USAMA BIN LADEN, the defendant, met with Co-conspirator and other members of Al Qaeda in

the Sudan, Afghanistan and elsewhere;

b. At various times from at least as early as 1991, USAMA BIN LADEN, and others known and unknown, made efforts to obtain weapons, including firearms and explosives, for Al Qaeda and its affiliated terrorist groups;

c. At various times from at least as early as 1991, USAMA BIN LADEN, and others known and unknown, provided training camps and guesthouses in various areas, including Afghanistan and the Sudan, for the use of Al Qaeda and its affiliated terrorist groups;

d. At various times from at least as early as 1991, USAMA BIN LADEN, and others known and unknown, made efforts to produce counterfeit passports purporting to be issued by various countries and also obtained official passports from the Government of the Sudan for use by Al Qaeda and its affiliated groups;

e. At various times from at least as early as 1991, USAMA BIN LADEN, and others known and unknown, made efforts to recruit United States citizens to Al Qaeda in order to utilize the American citizens for travel throughout the Western world to deliver messages and engage in financial transactions for the benefit of Al Qaeda and its affiliated groups;

f. At various times from at least as early as 1991, USAMA BIN LADEN, and others known and unknown, made efforts to utilize non-Government organizations which purported to be engaged in humanitarian work as conduits for transmitting funds for the benefit of Al Qaeda and its affiliated groups;

g. At various times from at least as early as

1991, Co-conspirator and others known and unknown to the grand jury engaged in financial and business transactions on behalf of defendant USAMA BIN LADEN and Al Qaeda, including, but not limited to: purchasing land for training camps; purchasing warehouses for storage of items, including explosives; transferring funds between bank accounts opened in various names; obtaining various communications equipment, including satellite telephones; and transporting currency and weapons to members of Al Qaeda and its associated terrorist organizations in various countries throughout the world;

h. At various times from in or about 1992 until the date of the filing of this Indictment, USAMA BIN LADEN and other ranking members of Al Qaeda stated privately to other members of Al Qaeda that Al Qaeda should put aside its differences with Shiite Muslim terrorist organizations, including the Government of Iran and its affiliated terrorist group Hezballah, to cooperate against the perceived common enemy, the United States and its allies;

i. At various times from in or about 1992 until the date of the filing of this Indictment, USAMA BIN LADEN and other ranking members of Al Qaeda stated privately to other members of Al Qaeda that the United States forces stationed on the Saudi Arabian peninsula, including both Saudi Arabia and Yemen, should be attacked;

j. At various times from in or about 1992 until the date of the filing of this Indictment, USAMA BIN LADEN and other ranking members of Al Qaeda stated privately to other members

of Al Qaeda that the United States forces stationed in the Horn of Africa, including Somalia, should be attacked;

k. Beginning in or about early spring 1993, Al Qaeda members began to provide training and assistance to Somali tribes opposed to the United Nations' intervention in Somalia;

l. On October 3 and 4, 1993, members of Al Qaeda participated with Somali tribesmen in an attack on United States military personnel serving in Somalia as part of Operation Restore Hope, which attack killed a total of 18 United States soldiers and wounded 73 others in Mogadishu;

m. On two occasions in the period from in or about 1992 until in or about 1995, Co-conspirator helped transport weapons and explosives from Khartoum to Port Sudan for transshipment to the Saudi Arabian peninsula;

n. At various times from at least as early as 1993, USAMA BIN LADEN and others known and unknown, made efforts to obtain the components of nuclear weapons;

o. At various times from at least as early as 1993, USAMA BIN LADEN and others known and unknown, made efforts to produce chemical weapons;

p. On or about August 23, 1996, USAMA BIN LADEN signed and issued a Declaration of Jihad entitled "Message from Usamah Bin-Muhammad Bin-Laden to His Muslim Brothers in the Whole World and Especially in the Arabian Peninsula: Declaration of Jihad Against the Americans Occupying the Land of the Two Holy Mosques; Expel the Heretics from the Arabian Peninsula" (hereafter the "Declaration of Jihad") from the Hindu Kush mountains in

Afghanistan. The Declaration of Jihad included statements that efforts should be pooled to kill Americans and encouraged other persons to join the jihad against the American "enemy";

q. In or about late August 1996, USAMA BIN LADEN read aloud the Declaration of Jihad and made an audiotape recording of such reading for worldwide distribution; and

r. In February 1998, USAMA BIN LADEN issued a joint declaration in the name of Gamaa't, Al Jihad, the Jihad Movement in Bangladesh and the "Jamaat ul Ulema e Pakistan" under the banner of the "International Islamic Front for Jihad on the Jews and Crusaders," which stated that Muslims should kill Americans -- including civilians -- anywhere in the world where they can be found.

(Title 18, United States Code, Section 2155(b).)

FOREPERSON

MARY JO WHITE
United States Attorney

Tab B

Speech delivered to Middle East Forum on September27, 2000, entitled "Prosecuting Terrorism in New York", reprinted in Middle East Quarterly, Spring of 2001.

The Middle East Forum Promoting American Interests

The Middle East Quarterly

SPRING 2001 • VOLUME VI

Prosecuting Terrorism in New York

by Mary Jo White

My topic concerns the international terrorism prosecutions of the Southern District of New York United Office (USAO) and New York's Joint Terrorist Task Force (JTTF); I also wish to say a little about my pe very complex problem of international terrorism in today's world. I speak not as a scholar, a philosoph policy-maker, but (more narrowly) as a prosecutor.

The Joint Terrorist Task Force

The Joint Terrorist Task Force celebrated its 20th anniversary of the founding by the FBI and the New Department (NYPD). The celebration was held (very appropriately) at the World Trade Center (WTC), t February 1993 terrorist bombing. With that bombing, international terrorism became an unwelcome dc New York and the United States.

As it happened, at the time of the World Trade Center bombing, I was the interim United States attorn the Eastern District of New York. But about two weeks later, I was nominated to become the United St the Southern District of New York where I had served as an assistant United States attorney from 197 case thus became one of my earliest and highest priorities. Little did I know that international terrorisr remain so prominent as a top priority throughout my tenure as United States attorney and result (so f international terrorism trials with two more to be held next year, including the trial involving the East bombings that took place in August 1998.

Before I go on, let me say a few words of tribute to the JTTF. The FBI and NYPD formed the JTTF in Ma a rash of unsolved bombings that occurred all over the city—at banks, missions to the United Nations, under cars—bombings being carried out primarily by domestic terrorist organizations operating in the Puerto Rican FALN group, various Croatian groups, an anti-Castro Cuban terrorist group called Omega I handled as an assistant United States attorney.)

The JTTF was created in response to this pressing law enforcement crisis. It was founded on the belief cooperation is essential to effectively tackle terrorism because the complex crime of terrorism cuts acr and must transcend agency rivalries. The JTTF now includes, in addition to the FBI and NYPD, the Bure Tobacco and Firearms (ATF), the Secret Service, the Immigration and Naturalization Service (INS), the Aviation Administration (FAA), the New York State Police, the U.S. State Department, the New York an Authority Police, the U.S. Marshals Service, the U.S. Customs Service, the Amtrak Police, the Suffolk C Department, the New York Metropolitan Transit Authority (MTA) Police, and the Naval Criminal Investig twenty years, the JTTF has been a huge success story, measured both in terms of arrests and convicti the public knows about and (even more important) in the mostly unseen work of the JTTF in detecting terrorist acts that do not result in prosecutions or publicity. In my opinion, members of the JTTF are tr city.

Terrorist Incidents Involving New York City

International terrorism has particularly affected New York City in recent years. It is a subject that the in New York have become all too familiar with, particularly since the terrorist bombing of the WTC on F leaving six people dead, over a 1,000 injured, and the entire population in New York City permanently way. That act of deadly aggression was all too quickly followed by the so-called "Day of Terror," a plot blow up the Holland and Lincoln Tunnels, the FBI's New York Office at 26 Federal Plaza, and the U.N. b of mass destruction foiled by the JTTF.

In short order, this frightening plan was followed by the "Manila Air Plot"—a horrific terrorist plot hatch Philippines by Ramzi Yousef, one of the masterminds of the WTC bombing and a fugitive from America was, in a single 48-hour period, to blow up a dozen U.S. jumbo jets belonging to such airlines as Delta Northwest, carrying mostly American passengers between the East Asia and destinations in the United Francisco, Portland, Oregon, Los Angeles and New York City. As many as four thousand persons could had this plot succeeded. It was foiled, largely due to the good fortune of a fire in the Manila apartment his fellow terrorists were building bombs to put on the planes. Shortly afterwards, Yousef was capture

returned to New York City to stand trial (separately) for the bombing of the WTC and the Manila Air plc that same time, the driver of the Ryder van that carried the WTC bomb to its destination was captured returned to New York for trial.

As a result of these events, our office has handled four major international terrorism trials:

· The 1994 trial of four defendants for the World Trade Center bombing;

· The 1995 trial of twelve defendants for the Day of Terror plot;

· The 1996 trial of three defendants for the Manila Air plot; and

· The 1997 trial of Ramzi Yousef and the driver of the Ryder van for the World Trade Center bombing.

All twenty defendants in these four cases, including Yousef, were tried and convicted by separate jurie: court downtown at Foley Square, each time with twelve New York citizens doing their duty and serving and difficult trials. Two different federal judges presided over these trials: Kevin T. Duffy and Michael E the United States District Court for the Southern District of New York.

These trials were followed by two other international terrorism cases. First, the FBI and New York law very soon called on to handle the investigation and prosecution of the nearly simultaneous terrorist bo 7, 1998, of the U.S. embassies in Nairobi, Kenya, and Dar as-Salaam, Tanzania, which tragically result both American and African citizens. Twenty-two defendants have been charged thus far with the emba broader conspiracy to kill American nationals living abroad. Six of the defendants are in custody in Nev pled guilty and five are awaiting trial.[1] Thirteen defendants, including Usama Bin Ladin, the leader of tl terrorist organization, remain fugitives; the investigation continues. The State Department has offered $5 million for information leading to the arrest or conviction of each of these fugitives; and Bin Ladin is Most Wanted list.

The investigation and prosecution of the East Africa embassy bombings and of the al-Qa'ida internatior organization headed by Usama Bin Ladin is likely to go on for years and result in a number of trials the conducted in the federal courthouse in Manhattan. The embassy bombings case is assigned to United S Leonard B. Sand. The initial trial of the six defendants in custody in New York is scheduled to begin on and is anticipated to last nine to ten months. We are seeking the death penalty against two of the defe

Second, Ahmed Ressam was arrested by U.S. Customs inspectors on December 14, 1999, as he attem a car loaded with hidden explosives and four sophisticated timing devices he had allegedly brought fro Seattle, Washington, on the public ferry. Ressam is purportedly a member of a terrorist network of Alg had plans to engage in terrorism just before and after New Year's Eve 2000. Ressam's case is being ha Seattle United States Attorney's Office. A defense motion to transfer Ressam's case from Seattle to Lo extensive pretrial publicity in Seattle was granted and the trial is currently scheduled to begin in March

Our office has charged two other defendants with providing material support for terrorists (primarily in identification papers, and airline tickets) in connection with the alleged bombing plot of Ressam. Our c before United States District Judge John F. Keenan, who is now considering pretrial motions. One of th charged in New York, who was arrested in Canada in January 2000, recently waived extradition and ha New York. An April 2001 trial date has been set for these two defendants.

Trying these many cases of international terrorism in New York City necessarily means, at least in the enhanced risk and security needs for the city. It also means an increased burden on the federal prison with housing, separating, and containing a number of high risk, maximum security prisoners awaiting prisoners need, and are entitled to, access to their lawyers, and the experts, translators, and discovery necessary for their defense. The security burdens especially on the U.S. marshals and the NYPD are al cases will mean a lot of hard work and personal sacrifices, both here and abroad, for not only prosecut the FBI, the NYPD—the entire JTTF—but also for our law enforcement and intelligence counterparts lite world because that is where the evidence is; that is where the suspects are; and that is where internal (directed especially at Americans) is being carried out.

Prosecuting Terrorists

How have we gotten to this point in New York? Does it make sense for New York City and the United S take on the burden of fighting international terrorists operating abroad? What are the unique features prosecuting international terrorists in American courtrooms? What else are we doing, and how else are combat terrorism, other than through law enforcement? How can we improve our effectiveness? These important and hard questions, which I'm not about to try to answer here.

But I do want to discuss very briefly the international terrorism cases we have investigated and prosec illustrate concretely how international terrorism has shrunk the world in a very unwelcome way and, u way that compels all of us—not only here in New York, but everywhere—to take the longer and broade our resources and resolve to try to prevent and combat terrorism wherever it occurs and in whatever f to do it without changing our own way of life or diluting our fundamental principles.

In many ways, prosecuting terrorists is not much different from prosecuting other violent criminals. Th same; the rules of evidence are the same; and, unlike in most other so-called civilized countries, terro charged and tried in the United States are accorded all of the rights and protections given to every oth defendant in our criminal justice system. That is how it should be. As proud as I am of the work of the office that led to the convictions in these cases, I am even prouder of them and our entire criminal jus

because, despite the extreme seriousness of their crimes, all of these defendants were given an emine accorded every measure of due process that our laws provide.[3]

Like all trials, each one of these recent terrorism trials has presented somewhat different challenges fo the judges, and the juries.

First WTC trial. Here the evidence was almost entirely circumstantial. There was no eyewitness to iden four defendants who were apprehended and tried; no insiders to testify; no defendants confessed or te was the vehicle identification number plate found early on in the bombing rubble which pointed to a pa that had been rented in New Jersey. And there were fingerprints, phone records, Ryder truck rental fo manuals, and chemical residues found in incriminating places, and even identifiable DNA from one def on an envelope containing a letter sent to *The New York Times* claiming credit for the bombing. Once p summation, all of these bits and pieces added up to a very powerful case to present to the jury, which defendants on all counts. All four of the defendants tried were convicted on March 4, 1994, and senten years in jail without the possibility of parole. (At the time of the WTC bombing, there was no applicabl penalty.) The convictions were affirmed by the Second Circuit Court of Appeals on August 4, 1998.[4]

Second WTC trial. Yousef and the driver of the Ryder van, who were fugitives at the time of the first tr after a separate trial in November 1997 and also sentenced to over 100 years in jail.[5]

Day of Terror trial. This was the trial of the defendants who plotted unsuccessfully to blow up New Yor public buildings; it was very different from the WTC bombing trials. The bomb plot having been foiled t the trial was basically a conspiracy trial. The JTTF had an informant who was able to infiltrate the terro He testified at trial how the conspirators had rented a warehouse in Queens where the terrorists went bombs—all caught on videotape and audiotape by the JTTF.

Some of these defendants, unlike the WTC defendants, did take the stand and testify, mostly claiming really building bombs over there in Queens but just training to fight in Bosnia. The defense also claime informant, who had been paid $1 million, was an Egyptian intelligence officer making up the evidence Egyptian authorities, who had themselves in the past charged, but failed to convict, the lead defendan involvement in the murder of former Egyptian president Anwar as-Sadat. That defendant is the blind c Abdel Rahman, who is now serving a life sentence after being convicted in New York for the Day of Ter with this Egyptian intelligence theme, the defense in the Day of Terror trial attempted to put America doing Egypt's bidding. The informant who had infiltrated the terrorist group had also secretly taped the NYPD detectives to whom he reported. The conversations were used by the defense to try to put the g enforcement on trial—an all too common tactic these days—for supposed infractions of the rules in an effort to get the defendants at any cost. The accusations were baseless, but the defense's attempted u information still provided lots of material for distraction.

At trial, Sheikh Abdel Rahman, the leader of an international radical Islamic movement, was proven to organization whose aim was to wage jihad, or holy war, of terror against the United States because he enemy of Islam and because he disapproved of the Middle East policies of the United States. After sev deliberations, the jury on October 1, 1995, returned guilty verdicts against all ten defendants remainin defendants had pled guilty during the trial.) On August 16, 1999, these convictions were affirmed by t

Manila Air trial. Unlike the earlier trials, this one is based almost exclusively on evidence obtained by f mostly in the Philippines; and nearly all of the witnesses were foreign. The involvement of foreign auth investigations and prosecutions that ultimately lead to charges tried in American courtrooms presents difficult issues—issues that we saw in the Manila Air case, will see again in the embassy bombing case future case involving terrorism committed abroad. It will most often be the case that either entirely, o foreign authorities will be the first on the terrorism crime scene and, at least initially, the primary ones investigation and any interrogations, obtaining evidence under their often very different rules and stan differences, although usually legally irrelevant, nevertheless give the defense the ability to appeal to t American jurors whose sense of fair play and justice is more naturally and instinctively defined in term law provides and approves.

In Manila Air, for example, there were allegations that one of the defendants who had confessed to Phi had been mistreated while he was in custody in that country. Tapes of portions of these interrogations law enforcement and, under our American rules of criminal discovery, were made available to the defe prosecution did not seek to introduce these statements at trial, but the defense did, in an effort to per none of the evidence gathered by foreign authorities should be trusted to serve as the basis for convic officers came, testified in open court, and were subject to lengthy cross-examination by the defense la

Obviously, questioning by foreign law enforcement agents of a suspect held overseas is beyond our co regulate, and in some countries the questioning may not be done the way the FBI would do it. It is als foreign officials present a convenient target for baseless allegations of mistreatment. Fortunately, jurie getting at the truth and, in the end, the Manila Air jury, on September 5, 1996, convicted all three def Ramzi Yousef, of all charges.

Plainly, if we are to effectively prosecute international terrorism cases, we must deal with evidence tha foreign rules and by techniques we in America don't use or necessarily approve of. We must work thro differences in law and practice with our international counterparts so that critical evidence is not comp legally or in its persuasiveness to an American jury.

Some further reflections on those trials: First, Yousef, the lead defendant in both the WTC bombing an although not a lawyer, represented himself *pro se* at the Manila Air trial, as is generally every defenda right in this country. We shouldn't be surprised to see this in international terrorism cases where very

will be more interested in making a political statement than in mounting the best defense to the charg about the impact on the jury of the dynamic of Yousef serving as his own lawyer—the alleged terrorist performing well) the role of lawyer and talking eyeball to eyeball with the jury. But we shouldn't have l perhaps some initial surprise at the judge's announcement that Yousef would be acting as his own law calmly went about their business, listened attentively and respectfully, sorted through all of the eviden their verdict.

Second, these terrorism cases have a special level of significance for investigators and prosecutors. Th because of the subject matter itself; it also results from the fact that even the least of these defendant and evidence—is capable of walking out of a courtroom and committing new terrorist acts. They would enhanced zeal and ruthlessness, and they would enjoy greater status in the terrorist world for having l American system of justice. Our criminal justice system is simultaneously respected and feared becaus system that cannot be fixed or corrupted. We must make sure that it continues to function fairly and e involving international terrorism.

Third, it is imperative, assuming we can obtain the evidence, to charge all who had a role in a terrorist leader, to the bomber, to the defendant who ordered chemicals or provided false identification papers facilitate a successful getaway. If we are to be effective, we must prosecute the foot soldiers as well as the best way to deter others from taking part in acts of terrorism. We must also continue to investigat prosecute every participant in every terrorist crime, however long that may take.

Fourth, many of the terrorist crimes prosecuted by our office were committed by convicted defendants Islam, a very honorable worldwide religion that was demeaned by these defendants and their crimes. the defendants' religion, are obviously the object of our prosecutions and investigations; we will contin terrorists and prosecute terrorist crimes, irrespective of their motivation.

Finally, none of us should ever confuse being vigilant, vigorous, and prudently enhancing security with fundamental principles and way of life as a free, open, and tolerant society. That is what we are all abc city, and we can't allow any terrorist attack or threat of terrorist attack to change that. For then the te won.

Protection from Future Attacks

The investigations in all of our office's terrorism cases continue, and we have indicted fugitives who re apprehended. While we can't possibly round up, prosecute, and incarcerate for life, or obtain the death every international terrorist wandering the globe bent on doing horrific harm to Americans, it would be reality, in my view, for us ever to think that it would be safer or wiser to just leave them abroad or sir get them away from the United States. The dangers to Americans and American interests do not stop borders but are worldwide, and the law enforcement response must also be worldwide.

Let me be more specific: one of the most chilling facts that came out during the Manila Air trial was pa Ramzi Yousef gave to the FBI and the Secret Service on the plane bringing Yousef back from Pakistan apprehended. Although Yousef was willing to talk—even brag—about the Manila Air bombing plot, he w the nature or formula of the bombs to be used or how they could be gotten through airport security be Yousef, there were still trained confederates of his who could and would carry out the planned bombin airliners. Yousef living in the Philippines or Ressam in Canada did nothing to protect Americans from th should we think that terrorist attacks on Americans and American interests abroad aren't really our pr responsibility here at home. That would be myopic, for we increasingly work, travel, and live abroad, s must just as vigorously seek to combat the ravages of international terrorism committed abroad again American interests as we do when the terrorism is directed at targets within the domestic boundaries

Will successful and firm law enforcement responses against international terrorism deter other terroris and believe that this has significant deterrent value. But we are not naive so we must and do expect si future. The embassy bombings in East Africa in August 1998 occurred after the trials and convictions i did the terrorist bombings directed at our American troops in Saudi Arabia, as did Ressam's ferry trip crossing the Canadian border into Seattle.

The sad fact is, many terrorist groups view America as the "Great Satan." Terrorist leaders issue *fatwa* Islamic law) that bless or even command attacks on Americans. The entire U.S. information, financial, communications infrastructure is at risk for terrorist attacks. The FBI and other parts of our governme the business community, are vigorously dealing with these risks, but we must all recognize that the Ur will remain a primary global terrorism target for the foreseeable future. It is also an unfortunate but c matter what we do, we cannot prevent every terrorist act directed at us, either at home or abroad.

To make matters worse, terrorist groups are more and more joining together to attack us as their com enemy. The Bin Ladin/East Africa embassies bombing indictment, for example, alleges involvement by Qa'ida, al-Jihad, and the International Islamic Front. Increasingly, we should expect to see such joint terrorists and terrorist groups coming together to launch terrorist attacks.

Conclusion

This reality—that we cannot prevent all future terrorist attacks—has three main implications.

Cooperation. There is also a continuing need for strong, global, international law enforcement investig prosecutions of international terrorists and terrorist organizations. This has occurred in the Manila Air dramatically, occurred and is still occurring in the embassy bombing case with the FBI and the JTTF w with their counterparts in Kenya and Tanzania to find, apprehend, and bring to justice each and every horrific crimes. The message and importance of such strong international cooperation is clear: If you c

anywhere in the world, the world, with some notable exceptions, will pursue you, using every lawful m and bring you to justice, no matter how long it takes.

We must also work with state and local officials and the business communities throughout the United S our ability to respond to any terrorist attack, wherever it occurs and whether it involves conventional v of mass destruction, or chemical or biological attacks. New York City, not surprisingly, is a leader in pr

Leadership. Tackling international terrorism requires a global effort that naturally calls upon the United a leadership role. And it is a role that we must forcefully and consistently exercise if we are to begin to combating and reducing the risks of terrorism, both at home and abroad.

Activism. Arrest and prosecution are obviously only two of the many tools to combat international terr powerful tools that have been successful and which we must continue to use. What do you do with a R tells the FBI on the plane bringing him back from Pakistan that his objective had been to topple the tw WTC into each other so that the death toll would exceed those killed in the bombing of Hiroshima durir failed in that objective, he says, because he ran out of money, this time, to build a big enough bomb. You use every tool in the counterterrorism arsenal—military, diplomatic, seizure of assets, and prosecu and stop the Ramzi Yousefs of the world.

We must recognize the threat international terrorism poses and not be oblivious, naïve, or passive, or unfounded criticism, and shy away from vigorous investigations and prosecutions of terrorists. All of us to take all reasonable, lawful measures to combat and safeguard ourselves from terrorism. That New Y leader in this effort is not something that it chose to do, any more than we chose to be the site of the it is a role that we must continue, so long as international terrorism remains a threat, and so long as N landmarks, institutions, and financial and governmental centers remain such attractive potential target

Mary Jo White is the United States attorney for the Southern District of New York, an area that New York City. This article derives from a talk she delivered to the Middle East Forum's lecture New York on September 27, 2000.

[1] Four of those were captured abroad and returned to New York to stand trial (two were returned from South Africa, and one from Germany); two were arrested in the United States; and three additional de custody in England where we are seeking their extradition.

[2] Those going on trial in January are Wadih El-Hage, a naturalized U.S. citizen born in Lebanon; Mohar Al-'Owali, a Saudi Arabian; Khalfan Khamis Mohamed, a Tanzanian, and Mohamed Sadeek Odeh, a Jor convicted, Mohamed and Al-'Owali could face the death penalty.

[3] In this regard the concluding remarks of the Court of Appeals in affirming the convictions were partic "The ten defendants were accorded a full and fair jury trial lasting nine months. They were vigorously counsel. The prosecutors conducted themselves in the best traditions of the high standards of the Offic States Attorney for the Southern District of New York. The trial judge, the Honorable Michael B. Mukas extraordinary skill and patience, assuring fairness to the prosecution and to each defendant and helpfu His was an outstanding achievement in the face of challenges far beyond those normally endured by a States v. Rahman 189 F.3d 88 (2d Cir.), cert. denied, 120 S.Ct. 439 (1999), 160, (2d Cir.), cert. denie (1999).

[4] United States v. Salameh, 152 F.3d 88 (2d Cir. 1998), cert. denied, 525 U.S. 1112 (1999).

[5] United States v. Ramzi Yousef, 93 Cr. 180 (KTD).

***To receive articles regularly by email, join the* MEF News *mailing list*.**

Printer-friendly version Email this article to a friend

Related Items

- Other items from the Spring 2001 *Middle East Quarterly*

Tab C

SDNY indictment against Usama bin Laden, the al Qaeda leadership, and twenty-two defendants for the East Africa Embassy bombings on August7, 1998.

[This document is voluminous and is being retained in the Joint Inquiry Committee's files.]

TESTIMONY OF MARY JO WHITE, FORMER UNITED STATES ATTORNEY FOR THE SOUTHERN DISTRICT OF NEW YORK

Ms. WHITE. Mr. Chairman, members of the committees, thank you for inviting me to testify before you in this very important joint inquiry. It goes without saying that the terrorist attacks of September 11 profoundly affected and changed each one of us and our Nation forever. But the most grievously impacted are obviously the loved ones of those who were so wantonly murdered that day without warning. It is to them that we most owe whatever answers there are to be found for how it happened and the assurance that we as a government have done and will continue to do everything in our power to prevent such human devastation from ever happening again.

My limited knowledge on this very complex subject of international terrorism I am honored to share with you for whatever use it may be to your inquiry. I have submitted a written statement which has been made part of the record, and I will just in my oral comments highlight a few of the points in the written statement. I would then be pleased this afternoon to answer any questions the committee has of me today or in the future as your work goes forward.

To give just a little bit of context to start, let me describe briefly the international terrorism investigations and prosecutions of the United States Attorney's Office for the Southern District of New York. From the beginning of my tenure as United States Attorney in June 1993 to its last day in January of 2002, I, together with a number of extraordinarily dedicated and talented Assistant United States Attorneys, agents and detectives from the FBI, the New York City Police Department, Joint Terrorist Task Force, JTTF, were actively involved in the investigation and prosecution of international terrorists and terrorist organizations who were plotting to attack or had actually attacked Americans and American interests both in the United States and abroad. No work in our office had a higher priority.

International terrorism work of the Southern District of New York United States Attorney's Office began with the investigation and prosecution of those responsible for the bombing of the World Trade Center on February 26, 1993, in which six people were killed and over a thousand injured. The work also included the investigation and eventual indictment of Usama bin Ladin, the leader of the al-Qa'ida terrorist network, indicted first in June 1998 for conspiracy under seal before he or al-Qa'ida had massively attacked anyone. A copy of that indictment is included with my statement, Mr. Chairman.

Bin Ladin and 22 other defendants were subsequently indicted in November 1998 for their role in the bombings of the U.S. embassies in East Africa on August 7, 1998, in which 224 totally innocent people, including 12 Americans, lost their lives.

In addition to the prosecution of those who bombed the World Trade Center in 1993 and those who bombed our embassies in Nairobi, Kenya and Dar es Salaam, Tanzania in 1998, the Southern District of New York United States Attorney's Office also successfully prosecuted approximately 20 additional terrorist defendants for their roles in three other major terrorist plots which were

fortunately thwarted by law enforcement: The 1993 Day of Terror plot to blow up government buildings and other structures in New York City, the 1994 Manila Air plot to blow up a dozen U.S. jumbo jets flying back to America from the Far East, and then the December 1999 Millennium plot of Ahmed Ressam, an Algerian terrorist trained in al-Qa'ida camps in Afghanistan, to detonate a bomb at the Los Angeles Airport.

In 2001, the Seattle United States Attorney's Office successfully prosecuted Ressam and the Southern District of New York office successfully prosecuted two defendants who from New York provided material assistance to Ressam's plot in the form of money, credit cards and phony identification papers.

In all, the Southern District of New York United States Attorney's Office charged and convicted over 30 defendants for international terrorism. There were no acquittals. All of the defendants are serving life or very lengthy prison sentences without the possibility of parole. There are, however, fugitives still at large in several of the cases, including bin Ladin himself, who as of September 11 had been under indictment for over three years and on the FBI's 10 most wanted list for approximately the same amount of time.

Fifteen of the 22 terrorists on the most wanted terrorist list announced by President Bush on October 10, 2001 are fugitives in the Southern District of New York cases—13 from the embassy bombings case, including not only bin Ladin but much of the leadership of the al-Qa'ida terrorist organization; one defendant from the 1993 bombing of the World Trade Center, Abdul Rahman Yasin, who fled New York like Ramzi Yousef did on the day of the 1993 Trade Center bombing and who, as you may have seen, was recently interviewed on 60 Minutes in a broadcast televised from Iraq; and one defendant from the Manila Air plot, Khalid Shaykh Mohammed, who has been widely reported in the media to be one of the major planners of the September 11 attacks.

I will speak to when the threat of international terrorism was regarded as a threat to America and explain the particular importance in all of this to the Day of Terror plot. Certainly by the time our embassies in East Africa were bombed in 1998, we as a government knew a great deal about the threat posed by bin Ladin and al-Qa'ida to America, and at least by the time of the embassy bombings indictment filed in 1998 much of that knowledge was indeed a matter of public record. But the high risk that international terrorism and terrorists posed to America, both in America and abroad, was known and appreciated as a significant threat from at least 1993.

The bombing of the World Trade Center on February 26, 1993 itself, of course, represented a dramatic incident of international terrorism that Ramzi Yousef, one of its masterminds, had brought from abroad to America. But it was, at least for us, the follow-on terrorist plot in 1993, the Day of Terror plot, to blow up in a single day the Lincoln and Holland Tunnels connecting New York and New Jersey, the George Washington Bridge, the United Nations and the New York FBI Office in Lower Manhattan that led us in the Southern District of New York United States Attorney's Office and the FBI to conclude that international terrorism was a long-

term, highly dangerous risk to the safety and national security of the United States.

The FBI and other public officials testified to this risk and spoke about it publicly to citizens groups. Prior to September 11, I also personally gave several talks discussing specifically the point that international terrorism had come from abroad to America and posed a significant continuing threat to America, both at home and abroad. A copy of one such talk is included with my written statement.

The Day of Terror plot headed by the blind cleric and leader of the Gama'at terrorist organization, Shaykh Omar Abdel Rahman, was fortunately foiled by the New York FBI and the JTTF because they had been able to infiltrate that terrorist cell, which was operating in the New York-New Jersey metropolitan area, with an informant posing as an explosives expert. As a result, that plot could be and was carefully monitored and stopped before it could come to fruition. The evidence necessary for the successful prosecution of Shaykh Rahman and 11 of his followers was also obtained. It was, in short, a very successful prevention and prosecution effort by the New York FBI and the Joint Terrorism Task Force.

The Day of Terror plot case thus illustrates one point I do want to make today, and that is, at least from our perspective, we viewed the terrorist investigations and prosecutions we did from 1993 through 2002 as a major prevention tool. Everyone's goal was to thwart plots before they occurred and to neutralize dangerous terrorists so that they could not attack in the future. In that effort we worked very closely with the FBI and especially later the CIA and other intelligence agencies to ensure that the first priorities were always prevention and national security. When criminal investigations and prosecutions could aid the overall national security effort, our office willingly and aggressively offered our help.

From my vantage point, the counterterrorism strategy of our country in the 1990s was not, as I have read in the media and heard a little bit of today, criminal prosecutions. Rather, as I saw it, criminal prosecutions were one tool in our counterterrorism efforts, a tool that certainly neutralized for life a number of very dangerous international terrorists, including Ramzi Yousef, a mastermind of the 1993 Trade Center bombing and the architect of the Manila Air plot as well as Shaykh Omar Abdel Rahman, the leader of the Day of Terror plot and head of the Gama'at terrorist organization that later joined forces with al-Qa'ida.

It was also, of course, our hope that the indictment of Usama bin Ladin and the leadership of al-Qa'ida in 1998 would result in the apprehension and neutralizing of these and other terrorists who posed and still pose very grave threats to the safety of America and the world. But none of us considered prosecutions to be the country's counterterrorism strategy or even a particularly major part of it.

In addition to cementing our view that international terrorism posed a significant threat to us here at home, the Day of Terror plot was also important for some other reasons. First, it showed the foothold that international terrorists had and were gaining in the United States. All of the defendants in the case were residing in New York and New Jersey. Some were here in the United States

legally. Some were here illegally. I should say that there is no doubt in my mind that it is a critical matter of national security that our immigration policies and procedures be dramatically enhanced.

A number of the terrorist defendants in the Southern District of New York cases, including Ramzi Yousef, for example, entered the country illegally. Others remained in the country illegally after they had come in legally, only to surface when they participated in a terrorist attack in the United States like the bombing of the World Trade Center. The shaykh himself, the leader of the group, was preaching his anti-American rhetoric in 1993 in mosques in Brooklyn, New York and Jersey City, New Jersey.

Secondly, and even more importantly, the Day of Terror plot illustrates the importance of the infiltration of terrorist cells by human sources and informants. Such infiltration is in my view one of the most effective means of preventing terrorist attacks. It is not easy to do. There are significant language, cultural and expertise barriers that must be overcome. Nevertheless, in my view, whatever can be done to enhance the FBI's and the Intelligence Community's ability to develop human sources and operatives capable of infiltrating terrorist cells should be done both in the United States and around the world.

At the conclusion of the trial of the Day of Terror plot, which was in 1995, I made the decision to form an International Terrorism Unit in the Southern District of New York United States Attorney's Office and to staff it initially with those half dozen Assistant United States Attorneys who had been involved in the investigations and prosecutions of the 1993 Trade Center bombing, the Day of Terror plot, and the Manila Air plot. To my knowledge that terrorism unit was the only one in the United States Attorney's Office prior to September 11. I personally supervised our terrorism unit.

I made the decision to establish a permanent terrorism unit because we had concluded that the risk of future terrorist attacks and plots was high and long term and because, as a result of the knowledge we and the New York FBI and JTTF had gained as a result of the two back-to-back 1993 international terrorism cases, we had of necessity amassed a great deal of intelligence about various terrorists and terrorist networks that we did not want to lose as we went forward. We wanted to pursue all leads of other terrorist conspiracies and attacks.

So, unlike with most other kinds of prosecutions, we did not close up shop after the Day of Terror plot defendants were convicted and went to jail. We did not wait for the next attack. We, together with the FBI and the JTTF, actively continued to investigate other possible terrorist crimes and conspiracies to try to learn more, to follow any lead that suggested itself. While it is certainly the reality that not every terrorist attack can be prevented, our objective and priority must always be a perfect prevention success rate. We must do whatever is lawful in our effort to achieve that.

You have asked in your letter to me about the role and effectiveness of criminal prosecutions in the fight against international terrorism. I think, as the Southern District of New York cases demonstrate, criminal prosecutions of terrorist defendants have been and can be effective tools to deal with terrorists who commit Fed-

eral crimes and as to whom there is sufficient available evidence to prove such defendant's guilt beyond a reasonable doubt under the rules governing criminal trials in the American criminal justice system. Prosecutions can also lead and did lead to cooperating defendants who provided invaluable intelligence on the terrorism threat as well as trial testimony.

These prosecutions also neutralized for life or many years a number of very dangerous terrorists who would have otherwise continued to commit further terrorist acts. Some bombs were thus undoubtedly not built and detonated. Some planes were not blown up. And some people were not assassinated. That is obviously a good thing. But criminal prosecutions are plainly not a sufficient response to international terrorism. For that, we plainly need more comprehensive measures and most especially a strong and continuing military response. That is my view today and that was my view prior to September 11.

Just as one example, and I will only give one of the limitations of the criminal justice system in dealing with international terrorism, criminal prosecutions of international terrorists have limited deterrent effect. When thousands of international terrorists all over the world are willing, indeed anxious to die in the service of their cause, we cannot expect prosecutions to effect significant deterrence. Each of the Southern District of New York cases I have mentioned in my statement followed the one before it, culminating most recently in the attacks of September 11. Prosecuting and convicting Ramzi Yousef for the 1993 World Trade Center bombing and the Manila Air plot did not deter other terrorists from bombing our U.S. embassies in East Africa in 1998 or from hijacking and flying those planes into the World Trade Center and the Pentagon on September 11.

You have asked also about the sharing and dissemination of information related to the threat of international terrorism. Your question is whether prior to September 11 the information about international terrorism gathered by the various parts of our law enforcement and intelligence communities was shared and disseminated sufficiently. This is one of many areas where I must defer to others who have the complete picture.

While we certainly had concerns about this issue in our office, my general impression was that the information and evidence developed in at least the terrorism investigations and prosecutions in the Southern District of New York was generally shared by the FBI with the Intelligence Community and other parts of our government as well as with local and State authorities. Much of the information was in fact developed by the Intelligence Community, and local and State agencies worked directly on the JTTF, which worked each of the Southern District of New York cases.

I cannot speak to what information the Intelligence Community may have had that was not shared with the FBI or law enforcement generally, if any, but I can say that the relationship was a very positive and cooperative one. The CIA in particular was of invaluable assistance in the Southern District of New York cases and investigations. I can also say from my personal experience as a prosecutor and U.S. attorney for many years that under the leadership of FBI Director Louis Freeh and Director George Tenet of the

CIA, the working relationship and cooperation between the FBI and the Intelligence Community at the highest levels was excellent and, even more importantly, we saw a sea change of improvement in the 1990s in the ranks of the agencies as well. Nowhere, nowhere, was this cooperation more apparent and productive than in the investigation of the terrorist threat posed by al-Qa-ida and Usama bin Ladin.

One other question on information-sharing that I should speak about, and that is whether the grand jury secrecy rules embodied in rule 6(e) of the Federal Rules of Criminal Procedure prior to their amendment by the USA PATRIOT Act impeded the sharing of information between the law enforcement and the Intelligence Community. My view is that rule 6(e) was not a significant barrier to the sharing of information developed in the Southern District of New York cases and prosecutions. It could have been, but it was not.

Grand jury secrecy rules do not appear to me to have impeded the sharing of information in the Southern District of New York investigations and prosecutions for several reasons. First, the vast majority of information obtained was not obtained through the grand jury but by non-grand jury means of investigation to which the grand jury secrecy rules do not apply. Second, if any relevant information was obtained through the grand jury to which rule 6(e) might apply, we were generally, and I think always actually, able to obtain it through alternative means as well so that it could be shared. Third, quickly over time the information we and the FBI obtained in our investigations became a matter of public record through publicly filed indictments and other court documents as well as public trials with detailed written transcripts and publicly filed exhibits. I illustrate what I am saying now in my longer written statement about the East Africa embassy bombing indictment in 1998 and all the things that were publicly known in 1998.

One final point on this: Our constant mind-set in the U.S. Attorney's Office was to try to maximize the sharing of information real-time so that it could hopefully be used by others to gain further information and, most importantly, to be used to possibly detect terrorist plots and to safeguard against any threats posed.

This leads me to my final point about information-sharing, but in the other direction, and I have to say if I were to single out the most significant concern that I had about our counterterrorism efforts prior to September 11, dating from at least 1995, it was that I feared we could be hampered in our efforts to detect and prevent terrorist attacks because of the barriers between the intelligence side and law enforcement side of our government. Some of these barriers were and perhaps still are statutory. Some were and perhaps still are cultural. Some were and still are court imposed. Some were and may still be voluntarily imposed by the agencies by way of guidelines to assure compliance with all legal requirements and to make an adequate record of such compliance.

Our Intelligence Community is charged with gathering foreign intelligence to protect the national security. The FBI has a foreign counterintelligence function and law enforcement, or criminal function. Historically, those functions have been separately staffed. International terrorism, however, cuts across both of these func-

tions. It does not fit as neatly into one category or the other as espionage may have during the Cold War. Much of the information gathered by the Intelligence Community is most often also evidence of a possible criminal conspiracy or other crime. Much of the information gathered by law enforcement as evidence of a terrorist-related plot is also most often foreign intelligence information relevant to the national security.

Yet at least as things were done in the 1990s through September 11, as we perceived it, that evidence, if gathered on the intelligence side, could not be shared with prosecutors unless and until a decision was made in the Justice Department that it was appropriate to pass that information over the wall to prosecutors either because it showed that a crime had been committed that needed to be dealt with by an arrest or further overt investigation or because evidence of such crime was relevant to an already ongoing criminal investigation.

Because of this structure and these requirements, I do not know even today what evidence and information might have been relevant to our international terrorism investigations that was never passed over the wall. I don't know if there is any, but I don't know that there isn't any either. To make a decision to pass information over the wall requires in the first instance a recognition of what that information is and what its significance is. In the area of international terrorism, this is a very difficult task, made more difficult by a combination of language and cultural barriers, coded conversations, literally tens of thousands of names of subjects that are confusing and look alike, and an unimaginably complex mass of snippets of information that understandably may mean little to the people charged with reviewing and analyzing the information and deciding whether to recommend that it be passed over the wall. A prosecutor or criminal agent who as it happens has for many years been investigating particular terrorist groups or cells and who has thus amassed a tremendous body of knowledge and familiarity with the relevant names and events might well recognize as significant what seems to other conscientious and generally knowledgeable agents or lawyers as something essentially meaningless.

What can happen, and I fear may have happened, but I don't know that, is that some relevant information that could have been passed over the wall wasn't and thus an opportunity could have been lost to make a connection that might have led to a further investigative step that might have led to the detection of an ongoing terrorist conspiracy.

We must, in my view, do everything conceivably possible to the eliminate all walls and barriers that impede our ability to effectively counter the terrorism threat. If policy and culture have to change to do that, they must change. If the law must be changed to do that, I would change the law. Indeed, I believe the Justice Department and the Congress thought that the law had been changed to help address this problem by the USA PATRIOT Act. A recent decision by the Foreign Intelligence Surveillance Act court, the FISA court, now on appeal, however, suggests otherwise. The FISA court decision also alludes to certain enhancements to the wall that the FISA court imposed prior to September 11, effec-

tively making the court the wall in certain international terrorism investigations.

The walls that so concerned us throughout my tenure as United States Attorney thus were built higher prior to September 11. While we were not made privy to the full rationale for this decision because we are on the other side of the wall and we certainly would not condone any misrepresentations, inadvertent misrepresentations to any court or any abuse of the FISA authority, raising the walls did concern us greatly from a public safety point of view. We voiced those concerns with officials of the Department of Justice prior to September 11. We do not know what, if any, relevant information was kept behind those walls.

Incidentally, when I was asked after September 11 by the Justice Department and FBI Director Bob Mueller what legislative changes we would recommend, we made a number of recommendations, but what I said was the single most important point is to get the walls down between the intelligence and the law enforcement communities. That remains my very strong view today. In my written statement, I offered a number of other recommendations, but the single most important recommendation I would make to the committees would be to address the full range of issues presented by the bifurcation of the intelligence and law enforcement communities and functions as they operate in international terrorism investigations, including the permissible use of FISA and the dissemination and use of the product of FISA searches and surveillances.

And so I will end there by thanking you very much for this opportunity to share my perspective and concerns. Thank you.

Chairman GOSS [presiding]. Thank you, Ms. White. That is very helpful. For those who have testified while we were out of the room in part or in total, our apologies for having the voting scheduled the way it is. It has left a time bind.

I am advised that we knew ahead of time that Senator Rudman had to leave at 1:00, so I am going to ask the indulgence of the members and our guests to switch the order slightly. What I would like to do, Dr. Pillar, is save your remarks till after lunch—and we start at 2:00 with your comments—and allow the Members who are here, using the abbreviated procedures that we have, to ask any questions of Senator Rudman that they may have in order to take advantage of his testimony.

That would mean, Judge Freeh and Ms. White, that questions that we would have for you would be also postponed until after Dr. Pillar's presentation this afternoon. Does that cause any angst to anybody on the panel? If there is no objection from Members, then we will proceed that way. And if I could have the list of the questioners, I think, Mr. LaHood, I am going to call these in order for again questions for Senator Rudman and I am going to do it in order, in the order we usually use, but I would ask Members, understanding we have only got 20 some minutes, so we will only have one question each on this, if that is possible.

Representative LaHood, you are recognized, sir.

Mr. LAHOOD. Senator, thanks so much for the enormous service that you have given to our country, not only in the United States

Senate but to these other issues that you have been so intimately involved with.

The one question that I would have of you, there is an idea floating around here which was actually adopted by the United States Senate on an amendment to Homeland Security with more than 90 votes to establish a blue ribbon commission dealing with 9/11. I have been opposed to this idea of a commission. I will just state that for you, but I would be very interested in knowing your views on this idea of establishing a so-called blue ribbon commission to look at what happened with 9/11 and make recommendations for the future.

Mr. RUDMAN. I have been asked that a number of times and, frankly, I go back and forth, because I think there are a lot of things that have to get done and I think a lot of us know what has to get done and we ought to get about doing it, and commissions tend to postpone actions sometimes and that is not good.

The other problem, though, that you face is that my sense from traveling around the country and speaking is the American people really don't think yet that the Congress has fully explored all of the events that have happened. I don't agree with that. I think a lot of that is happening here. I think a lot of it has happened in the Judiciary Committee and other committees of the Congress. But the bottom line is that you have got a constituency out there that you are going to just have to decide whether or not they will feel this government is being open enough with the hearings that have been public as opposed to a commission.

If I were here today and had to cast a vote, I won't give you the this hand or the other hand answer, I guess I would vote for the commission to make the American people feel the Congress isn't hiding anything, is baring everything, the American people will learn exactly what happened, though frankly I think they know pretty much what we know by now. That is my own view.

Chairman GOSS. Senator Feinstein.

Senator FEINSTEIN. Thanks very much, Mr. Chairman. Senator Rudman, let me ask you this question.

Former Director Freeh I think made a very compelling case on what the FBI has accomplished in many of these investigations. As one that has looked into both sides of this, from the FBI law enforcement perspective, the CIA intelligence perspective, some have written, and later on in my more extensive questioning I am going to talk a little bit about William Odom's views on this, that the culture of the FBI is so indigenous as a law enforcement agency that it really cannot be an effective intelligence-gathering agency. Do you agree with that? And if not, why?

Mr. RUDMAN. I do not agree with that. For background, Senator Feinstein, let me point out that as chairman of PFIAB, I had an occasion, a number of occasions, to call Director Freeh before the PFIAB as well as the Director of the CIA to look at these very issues that we are all talking about today. It is my view that the best domestic intelligence-gathering organization which is on the ground today is the FBI. They have their collection, if you will, in every field office. I don't know how many there are, Louis.

Judge FREEH. 56.

Mr. RUDMAN. There are 56.

Judge FREEH. 44 overseas.

Mr. RUDMAN. Plus there are the 44 overseas. This is the best collection that you are going to get domestically. Of course there are many other agents in other places. The problem has been, I think, not quite as you posed the question. The problem has been that they have had a law enforcement mind-set as they approach it. I think that Mary Jo White's testimony was extraordinarily useful in looking into how a U.S. Attorney in the most critical area of the country in this area had to look at this issue and how to deal with it.

To me it is not a question of trying to get a new agency to do the domestic intelligence, counterintelligence; it is a question of the resources that were asked for. I can tell you that in 1998 or 1999, Director Freeh came to me and asked me to enlist my support with people on the Hill to try to do some of the things that he felt at that time were necessary, and as I recall, they were personnel but they were also technology. It was the technology. They recognized they couldn't get a grip on all the information that was coming in.

I did try and they had some success but, for reasons we all understand, the Congress can't always do what agencies think are vital. But as you heard his testimony, I think the numbers, 800 requested and five granted in the account of money and technology, I don't think the Bureau was given the resources it needed during the mid- to late–1990s to develop the kind of intelligence efforts it needs. I think they can do it but they need a lot of resources, and I think Director Mueller has moved strongly in the right direction in taking what Director Freeh started and building on it to have truly a domestic intelligence unit that is strong on analysis. They have already got the collection.

So that would be my answer.

Senator FEINSTEIN. Thank you very much. Thanks, Mr. Chairman.

Chairman GOSS. Mr. Roemer.

Mr. ROEMER. Thank you, Mr. Chairman. Senator, nice to see you up here. Thank you for your help in the past as well, too, on many of these important issues. I want to thank you as well for your work on the commissions that you served on. I happen to agree with your bottom line that a new blue ribbon, independent commission is needed in this instance and I want to come back to your service on the commission that reported to Congress some very important findings.

One of the problems around Congress is that they don't implement some of the good recommendations made by very knowledgeable people in law enforcement, in public service, in intelligence-gathering that serve on these commissions.

In your testimony, you mentioned that a couple of Members had worked to implement the Homeland Security Department, which is now in a state of nowhere—we don't know what is going to happen to that—but I would appreciate just very succinctly three other high priority recommendations made by your commission that this Congress should act on and act on quickly.

Mr. RUDMAN. You are talking about the Hart-Rudman Commission?

Mr. ROEMER. Yes, sir.

Mr. RUDMAN. The Homeland Security, as you know, that department was our number one priority for the very kinds of things you have heard today about stovepipes, having to go over the wall with information. We have got 44 different agencies right now who have some piece of this. They have separate information technology. They have separate missions. That has to be brought under control.

I would urge the Congress and the administration to settle whatever disputes you have over these labor issues and please get this thing established, because frankly we haven't got anything done yet and until that gets deployed, it will take a year to a year and a half to get it working. So I think that is number one in priority.

The second priority I believe is starting to take form. If we have—it is not a question of if. When we have another terrorist incident in the United States, and we will have one, we have recommended in our report in great detail the fact that we have citizen soldiers in this country deployed all over America called the National Guard that are the best line of defense in terms of first response, because if we have a weapon of mass destruction in this country, no one other than the United States military will be able to respond and help citizens. They are the only ones who are trained, who have the equipment, who have the communications. The National Guard should be dually trained. They should have their regular mission, but there should be strong dual training in responding to terrorist attacks.

If something happened in New England, you have got the Guard units from all over New England that could focus on, let's say, Boston. In California you have got those from the western States, from Oregon, Seattle and the State of California. As we looked at these Guard units, we felt they really ought to be the core of the first response to major terrorist attacks, be it medical, communications, transportation, law enforcement. And so that would be my second priority.

My third priority is port security, which I just certainly hope that appropriate committees will start to take a look at. With all due respect, I'm a little tired of having my shoes taken off at LaGuardia Airport. I usually dress like this. I don't think I look much like a terrorist, and how many dollars have been spent examining my shoes I don't know. But I tell you this much, that 50,000 containers are coming in every day into every port in this Nation, 1½ percent are being inspected, who knows what they contain. It is a high priority, and the problem is something is going to happen and then we're all going to say, well, but we didn't know. Well, we did know and it is not only our commission that has made that statement.

Those are my three priorities right now.

Mr. ROEMER. Thank you.

Chairman GOSS. Senator Roberts.

Senator ROBERTS. Thank you, Mr. Chairman. Let me say, Warren, that your words of wisdom did not fall on deaf ears, at least in terms of the official report, which we hope hasn't simply collected dust. We have your report, Preparing for the 21st Century, the *Cole* Report, which just popped out here, what, a week ago, the Jeremiah Report, the CISI, Defending America in the 21st Century, the Gilmore Commission on Terrorism and the Bremer National

Commission on Terrorism and the Odom study, which was back in 1997.

I just tried to add up the similar recommendations by all of these commissions, and I think I have 95 recommendations.

Mr. RUDMAN. That is about right.

Senator ROBERTS. They were made in an early September closed hearing part of this official record, so we do have a good foundation. One of the things that I would like to ask you, you mentioned how many agencies were involved in regards to the agencies that think they have the jurisdiction in regards to terrorism and homeland security. I can't remember the number you just said. What?

Mr. RUDMAN. About 44.

Senator ROBERTS. We asked 46 a year ago July to come before some appropriators, the Intelligence Committee and the Armed Services Committee. This is some 15, 16 months ago. At that time there were 46. We asked them what their mission was, what they really did and who was in charge. At that time, according to my count, the staff, or my staff estimated there were 14 subcommittees and committees in the Senate alone that allegedly had jurisdiction. Since that time, we have been able to identify 80 Federal agencies who have some degree of jurisdiction in regards to homeland security and terrorism. I am not making this up. According to the leader, Tom Daschle, and also Trent Lott, or the leadership, there are 88 subcommittees and committees now that feel they have some jurisdiction.

It seems to me the Congress of the United States has a responsibility to get our act together just as we do in terms of trying to really coordinate homeland security. You are a former chairman of this outfit. It seems to me that we could possibly think about joining the House and Senate into a joint committee, not make it a select committee, make it permanent, reduce the numbers and tell the Members who serve on the Intelligence Committee they are limited to some degree with the outside committees upon which they serve. I'm not sure what we would have the term limits in there as well. What do you think of that?

Mr. RUDMAN. Senator Roberts, if you turn to either recommendation 49 or recommendation 50 of the Hart-Rudman Commission, you will find your words are embodied into a recommendation. We believe that the vastness of this jurisdiction over homeland security is so different than anything else the Congress has dealt with before that you must, you must, have a consolidation of committee responsibility for homeland security, certainly in both the authorizing and the appropriating area. It is absolutely essential.

If you don't, then whoever the new Director is, instead of spending time with these five and six new key agencies that are going to be coming into his new Cabinet department and giving them mission statements and building the kind of lateral communications you need and having the diversity of leadership you are going to need to move across these heretofore stovepipes, he is going to spend all of his time up here. He is going to be here all the time.

With all due respect, when I was here I used to sometimes wonder whether or not we weren't bearing too hard on the Director of the FBI or the Secretary of Defense. These people have to spend so much time up here. A lot of it is necessary. After all, the over-

sight comes from the Congress and I understand that. But in homeland security, unless you adopt some sort of a different plan with the House and the Senate, either jointly or each having one or two committees, I frankly think you are going to really cause enormous problems, not only time problems but frankly there is going to be a difference of opinion among all these committees about how certain things ought to be done.

So I would commend you look at our report, 49 and 50. It was a unanimous recommendation.

Senator ROBERTS. I looked at the report, and I introduced legislation and it is collecting dust.

Mr. RUDMAN. We appreciate it. As a matter of fact, Senator Roberts, I would thank you. You are one Member of Congress among five or six who came to the press conference in January of 2000—December—when we announced that report.

Chairman GOSS. Chairman Graham.

Chairman GRAHAM. Senator, as you said, the centerpiece of your recommendation was the establishment of a Department of Homeland Security. I think that is close at hand, but it is also going to be occurring at a time when we have intelligence information that indicates we might have additional risk as a result of what is happening around the world. In fact, earlier today the Director of Central Intelligence sent to this committee a letter in response to our request for further declassification of the National Intelligence Estimate that was issued last week.

In the letter, Mr. Tenet states, "Baghdad for now appears to be drawing a line short of conducting terrorist attacks with conventional or chemical or biological weapons against the United States. Should Saddam conclude that a U.S.-led attack could no longer be deterred, he probably would become much less constrained in adopting terrorist actions. Such terrorism might involve conventional means, as with Iraq's unsuccessful attempt at a terrorist offensive in 1991, or chemical and biological weapons."

So we are at a point that the threat level is up and we are about to pass this new department and you indicate correctly, maybe conservatively, that it is going to take some period of time for the new department to go through its transition period and be fully effective. With that as a predicate, any suggestions of what we should be doing in the early stages of this new department so that we don't have the unintended consequence of making us more vulnerable because of the almost unavoidable disruptions that such a major new reorganization entails?

Mr. RUDMAN. That is a very interesting question. I want to give you an answer because I have thought about it a bit, not in quite the way you phrased it. But let me put it this way.

One of the things that is vastly understood, certainly in the country and maybe in parts of the Congress, is that each of these agencies going into the Homeland Security Department is going to maintain its identity. The Coast Guard will still be the United States Coast Guard. FEMA will still be FEMA. INS will be INS. The Secret Service will be Secret Service. And the one or two others that they have added to our recommendations. What they are going to have the advantage of is being parts of one department with a common leadership and a common technology base.

I think it is very important that once this legislation passes, that the Congress in the transition section of the statute, either in report language or in statutory language, make it clear that these agencies are to continue to operate at their present levels of activity, in whatever their tempos are, irrespective of the fact they are being merged into the new agency. The merger can take place administratively but the people in the field who are doing the work cannot be deterred from what they are doing. That would certainly apply to the Border Patrol, the Coast Guard and the INS. I think it is a very good question. I don't think—as I remember the statute, there is nothing in there regarding that.

I think you get my point, that they better keep doing their job as they are moving into the new agency. It is like consolidating two fire departments. You want to make sure the engines are running while the transition is going on, lest the town burn down.

Chairman GRAHAM. If I could ask one more question along the same lines. It comes from one of the recommendations that Director Freeh made. It was number 10. He calls for establishing a Domestic Public Safety Office in the executive with responsibility for coordinating and supporting national law enforcement issues. There has been a proposal that within the Department of Homeland Security, in addition to creating the department, that an office similar to what Mr. Freeh has suggested be established in the White House in much the same way that after the 1947 National Security Act we created the National Security Council to be the coordinative agency and the most direct adviser to the President on national security issues.

Do you think we need within the executive branch, potentially within the White House itself, a Domestic Public Safety Office for similar coordinative and supportive functions?

Mr. RUDMAN. We now will have a Department of Homeland Security, but as I understand, the President intends to keep by executive order a homeland security unit within the White House. And you have got the NSC. I'm not sure if I agree with Director Freeh on that. I would have to think about it. The problem I have is when you start—if it was organized in the right way, maybe it would work.

But right now the person who ought to be doing that is the Attorney General of the United States, it seems to me. He ought to be the domestic security officer for the country. He is a member of the Cabinet, he is a statutory member of the National Security Council. I would think if the talents of that department are utilized properly, that he ought to be able to do it.

On the other hand, I have not sat where Louis Freeh has sat, so I don't want to criticize it. I worry about creating more czars, if you will, in the White House for everything, because they tend to have their authority diffused unless they have got budget authority, and none of them do. I'm kind of a little uneasy about that, but Director Freeh I am sure can explain it fully this afternoon.

Chairman GOSS. Thank you, Senator. Senator DeWine.

Senator DEWINE. Thank you, Senator, for joining us and all of the witnesses. You have been very, very good and helpful.

Senator, I think as a result of September 11 we on this committee need to reexamine at least and think about what our role

is in regard to oversight. I think those of us who serve on the Judiciary Committee need to do the same thing. I wonder what suggestions you might have specifically for this committee or for the Judiciary Committee.

Mr. RUDMAN. My sense, having served on this committee—I did not serve on Judiciary—is that if I had a criticism as I look at it then and now, I thought there were occasions we got down into the bushes too much, got too much into micromanaging what really have to be executive decisions.

I think there are some broad policy questions involving the Intelligence Community. They are serious questions. They are addressed in this report. They have been addressed in some of the reports that Senator Roberts spoke about. You kind of do what you like to do. It is probably—it is a lot more interesting going in closed session and talking about some of the covert operations than it is dealing with wiring diagrams of how things ought to be set up but, frankly, I don't know how this committee is run today, I only know how it was run when I was on it a number of years ago, and I thought sometimes we got into the detail too much with the agency. I really believe that there are serious structural issues which have to be battled out and on which there is substantial disagreement. In the final analysis, this committee and the administration will decide how those structures will take place. To me that is where the effort ought to be in my view.

Senator DEWINE. Thank you, Mr. Chairman.

Chairman GOSS. Senator Thompson.

Senator THOMPSON. Thank you, Mr. Chairman.

Senator, somewhat along those very lines that you have just been discussing, the issue of what part is the responsibility of the administration and what part is our responsibility as we tackle these issues, how much flexibility should they have, that really goes to the heart of where we are on the homeland security bill. You are right, it is bogged down right now and I am sure you have been following it, but for those who have not followed it real closely, it essentially has to do with two areas.

One is the authority of the President. Presidents since JFK, either through executive order or by statute, have had the authority to abrogate collective bargaining agreements in times of national security. Those who have a different view are insisting that there be additional criteria, that people moved into the new Homeland Security Department, that the President has to determine that their job function has essentially changed in order for him to be able to apply that authority. It is a difference.

Secondly, it has to do with the issue of flexibility, that the person, persons running the new department will or will not have. We are having a big battle up here as to whether or not we should essentially retain the same work rules, the same requirements in Title V across the board. Keeping all the worker protections, keeping all the whistleblower protections and all of the basic things, but in terms of pay, in terms of reward, discipline, termination, levels of appeal and all those things that were created, some of them 50 years ago, we are in a battle royal up here now as to how much flexibility and how much change we should have.

I noted in Director Freeh's testimony, and I would turn to it, in regard to half a dozen of the recommendations he makes, it has to do with these same kind of areas. Compensation, the number of people they need, staffing, exempt the FBI from compensation restrictions of Title V, procurement procedures, which is a part of the homeland security bill. Achieving interoperability, making all these 22 disparate agencies we are bringing in in the homeland security context work together, and restructure the budget to give more flexibility to the DCI, Attorney General and FBI Director to better allocate program funding—in other words, to put people and money where you need it and have some accountability at the top but also flexibility at the top, because we are living in a different age.

I guess you can see where I am leaning in terms of this debate, but I would appreciate your overall view from 30,000 feet or so, if you could, or any more detail if you have followed it that closely as to what direction we should be going in here or how we should resolve what essentially as of this moment has killed the homeland security bill for this year. The American people are going to have a hard time understanding the things I have just been talking about are going to be things that kill the homeland security bill this year.

Mr. RUDMAN. Far be it from me to give political advice, but I would not want to be a Member of Congress if you go home without passing that bill and something bad happens while you are on recess because people are going to think if they had only done the homeland security bill, things would be better off. Maybe they wouldn't have been, but the fact is the perception would be that you didn't do what you should do.

I can answer the question very simply, because the commission is on record. Hart-Rudman laid out very clearly that we believe that because of the national security nature of this particular organization, that there ought to be—we didn't lay them out specifically but there ought to be broad flexibility for that Cabinet Secretary in terms of personnel policies and we were very clear that they ought to be flexible and we made no bones about it—strong language, bipartisan, seven Democrats, seven Republicans. It was not a partisan issue.

What I have suggested to some people, and I am not sure where this debate is right now, why don't you simply take the identical provisions that applied to people at DOD and apply them to this agency. Maybe that is less than the administration wants, maybe that is more than some of those who think labor protections are inadequate, but it certainly seems to be a reasonable compromise. It has worked at DOD. So that would be my suggestion. I think I answered your question.

Senator THOMPSON. Yes, sir. Thank you very much.

Chairman GOSS. Ms. Harman.

Ms. HARMAN. Thank you, Mr. Chairman. Hi, Senator.

Mr. RUDMAN. Good morning.

Ms. HARMAN. As you know, I served on the Bremer Commission and have been passionate about this issue of homeland security for as long as I can remember. About an hour ago, in fact, I spoke to Governor Ridge about my view, echoing Senator Thompson, that more needs to be done to unstick this issue in the Senate. He tend-

ed to agree. I cannot imagine for the life of me why some reasonable compromise along the lines you are suggesting cannot be reached on this civil service issue. It was reached in the House. I'm not sure what we did was perfect, but the bill passed on a bipartisan vote at 4 a.m. in July in the House and we all expected something would happen in the Senate by now.

My question is this: From where I come in Los Angeles—and I was just there yesterday—people are much more concerned about the potential suicide bomber next door than they are about what Saddam Hussein may have in store for us in a year or so when he gains nuclear capability. Let's hope not. You have made a suggestion. Do you feel that there is a way to mobilize pressure now to get more good minds working on this now to get this bill passed in the Senate? My view would be vote on whatever version they may choose to be on and passed in conference and funded before Congress adjourns.

Mr. RUDMAN. First, let me thank you. I should have mentioned when I credited people with picking up on our suggestions you are in the forefront of that, and I guess I just didn't see you sitting there. Maybe you weren't there. But I want to thank you for what you did and continue to do. I frankly am a little bit appalled at the problem.

I have been involved in some intractable fights here in the Senate where we just couldn't seem to get going, but we eventually got it done. I have to believe it will get done before you leave here. It is just too important to leave undone.

I think a simple solution is to cut it down the middle and say if it's good enough for DOD, it's good enough for Homeland Security, and I think everybody ought to buy into that. That's my view. Maybe the administration won't, maybe some of the Congress won't, but I think it is a reasonable solution. It has worked there for all these years. The Secretary of Defense has a lot of flexibility in some areas. The Secretary of Homeland Security ought to have that flexibility.

That would be my suggestion, for what it is worth. I have been asked by both sides, by the way, to help on this and I have made a number of phone calls, but I am becoming—obviously as I get older my persuasive abilities are lessening.

Ms. HARMAN. I thank you. I know I can't ask another question, but some clear way to state that we do not intend to change existing law, existing law codified by President Carter and operating through five administrations, I would think would be the answer.

Mr. RUDMAN. Could well be.

Ms. HARMAN. Thank you, Mr. Chairman.

Chairman GOSS. Mr. Condit.

Mr. CONDIT. Thank you, Mr. Chairman. Senator, you've stated that you feel the DCI should have more authority. Right now in the Congress some of the committees are considering giving Under Secretary status to the Secretary of Defense to have an Intelligence Under Secretary. Do you think that is a good idea or a bad idea?

Mr. RUDMAN. I think it is a terrible idea. Secretaries of Defense have been trying to run the Intelligence Community in this town for 25 years and Secretary Rumsfeld is no exception. My friend Bill Cohen is no exception. It is a horrible idea and if you do it, you

might just as well dismantle the Intelligence Community as we know it and call it what it is, the Department of Defense.

Mr. CONDIT. You have left no doubt of where you are.

Mr. RUDMAN. I don't have any doubts.

Mr. CONDIT. Thank you, Senator. Thank you very much.

Chairman GOSS. It is wonderful to get a nonevasive answer, isn't it?

I want to thank all the members of our panel, Ms. White, Judge Freeh, and Dr. Pillar, who will be back this afternoon, particularly Senator Rudman who has been put through the extra paces already before lunch. We appreciate very much the time that you are taking out on this. It is valuable. It is helping us. I know that we have Member interests and Members will be back after lunch and we will continue on with questions after we hear from Dr. Pillar.

We have your testimony, anyway, as you know, so not all is lost, but we would like you to start this afternoon at 2:00 or as close thereto as we can get enough people back here.

Thank you very much. Thank you very much, Senator Rudman. We are in recess until 2:00.

[Whereupon, at 1:10 p.m., the Joint Inquiry Committee was recessed, to reconvene at 2:00 p.m., this same day.]

AFTERNOON SESSION

Chairman GOSS. Can I ask the committee to come back to order, please, and invite our guests to be seated. And we are going to start with Dr. Pillar, who is going to tell us a lot, I think, about terrorism, because, as I've said before, I think he is one of the great authorities. And if you haven't read his book, you should. The floor is yours, sir.

TESTIMONY OF PAUL R. PILLAR, NATIONAL INTELLIGENCE OFFICER FOR THE NEAR EAST AND SOUTH ASIA AND FORMER DEPUTY CHIEF OF THE COUNTERTERRORIST CENTER AT THE CENTRAL INTELLIGENCE AGENCY

Dr. PILLAR. Thank you, Mr. Chairman and members of the committees. I appreciate this invitation to testify and this hearing on lessons from past U.S. experiences in confronting international terrorism. And I commend the committees for holding a hearing with this particular focus. Reducing the chances of terrorist strikes against our Nation's interests requires examination not only of a single incident, however tragic and traumatic that is, but also understanding what has and has not been tried in the past, what changes in our approach have already taken place and what possibilities and limits have already been demonstrated.

One lesson from the past is that the principal characteristics of the terrorist threat we face today and the challenges for intelligence that those characteristic pose have been with us for quite some time. The difficulties that the September 11 case presented to intelligence and to law enforcement, for that matter, were all too typical of what we have repeatedly faced in the past. Terrorist groups or, more specifically, the parts of them that do the planning and the preparation for terrorist attacks are small, highly secretive, suspicious of outsiders, highly conscious of operational secu-

rity, and for those and other reasons extremely difficult to penetrate.

The collection challenges go even further. The intelligence target is not just a fixed set of targets. It is anyone, even if not a card-carrying member of al-Qa'ida or some other known terrorist group, and even if the person has not been involved in terrorist activity in the past, but anyone who may use terrorist techniques to inflict harm on U.S. interests.

Along with the collection challenges, are the analytic ones. The material that counterterrorist analysts have had to work with has always consisted of voluminous but fragmentary and ambiguous reporting, much of it of doubtful credibility, that provides only the barest and blurriest glimpses of terrorist activity. The analysts have long been faced with blizzards of flags or dots, call them what you will, that could be pieced together in countless ways. If pieced together in the most alarming ways, the alarm bell would never stop ringing.

Although the task of tactical warning has always run up against these formidable challenges, the scraps and fragments that intelligence collects often have enabled analysts to offer warning of a more strategic nature. But that terrorist threat from certain kinds of groups, or in certain countries or regions, or against certain categories of targets, or in response to certain kinds of events is higher than it is elsewhere. The result has been a persistent pattern in the Intelligence Community's performance on this subject that has been noted, for example, in the findings of the investigation that was led by General Wayne Downing into the bombing of Khobar Towers in 1996.

That pattern, an absence of tactical warning but good strategic intelligence of the underlying terrorist threat, is what you get when earnest efforts are played to extract what can be extracted from this extremely hard intelligence target. Certainly the Intelligence Community must spare no effort to obtain tactical intelligence on future terrorist attacks against U.S. interests.

But years of experience teach us that even if high priority is given, as it has been, to the development of sources for that kind of very specific information, and even if considerable imagination and resources are applied to that task, truly well-placed sources inside terrorist groups, the kind that can yield plot-specific information will always be rare.

A corollary lesson is that the United States should avoid overly heavy reliance on intelligence to provide tactical warning. The panel that was chaired by retired Admiral William Crowe and examined the embassy bombings in 1998 noted an unfortunate tendency in security managers towards such excessive reliance on tactical warning. Intelligence officers share a responsibility for countering that tendency by reminding consumers what we don't know as well as what we do. To borrow an advertising slogan, an educated consumer is our best customer.

As important as tactical warning is, it represents only a fraction of what intelligence has contributed through the years to counterterrorism, including contributions that have saved lives. Strategic forms of intelligence can be, in fact, even more useful than the tactical as inputs to decisions to security counter-

measures, many of which involve costly long-term programs to respond to continuing threats rather than to a single plot.

One subject that received strategic attention from the Intelligence Community in 1990 was threats to the U.S. homeland. The 1993 attack against the World Trade Center was certainly a key event. It did not generate anything close to the level of public attention and level of concern that we see eight years later, and that, of course, is the difference between an attack that kills six people and one that kills 3,000.

But to Intelligence Community analysts, the larger threat to the homeland was apparent in the bombing of the World Trade Center. Truck bombers in '93, after all, had been nothing less than to topple the Twin Towers and kill thousands in the process.

The community's work on this subject over the next couple of years culminated in 1995 in a National Intelligence Estimate, the most formal and fully coordinated form of intelligence assessment, one that is personally approved by the DCI and heads of the community agencies. The sole subject of this Estimate was foreign terrorist threats to the U.S. homeland. The FBI, along with CIA and other Intelligence Community agencies, participated fully in preparation of this Estimate so that it would reflect the Bureau's information on the foreign terrorist presence in the U.S. as well as the intelligence available to CIA and others.

This Estimate, as was noted in one of your joint inquiry staff reports, addressed civil aviation as an attractive target that foreign terrorists might strike in the United States. This particular aspect of the Estimate was the subject of subsequent efforts involving the DCI Counterterrorism Center, the FBI, the National Intelligence Council, and the FAA to sensitize relevant consumers to that particular threat. The FAA arranged, in fact, a set of special briefings for representatives of the aviation industry, at which senior CIA and FBI counterterrorist specialists like myself presented much of the material in the Estimate as part of an effort to persuade the industry of the need for additional counterterrorist security measures for domestic civil aviation.

I might also add I was proud later on to participate in, along with my Intelligence Community and FBI colleagues, in the work of the Gore Commission, which Mr. Freeh mentioned earlier.

What is the lesson to be drawn from this episode, apart from the direct one that the Intelligence Community, or, at least part of it, and the FBI were working closely with the relevant regulatory agency as early as the mid 1990s to call attention to the foreign terrorist threat to domestic civil aviation? I think it is that we, as a Nation, tend to be more willing to respond with expensive new security measures in response to past tragedies that have already occurred than to projections of threats that have not yet materialized.

The Intelligence Community certainly has an important duty here. As any new intelligence analyst is taught, what matters is not just to make correct predictions and hit the right notes, but to beat the drum loudly enough about impending threats to have some chance of making an impact on policy. In this instance, perhaps the Intelligence Community should have beaten the drum even more loudly than it did, but it is tough to compete with what

had been, right up until September 11, many years of civil aviation operations in this country that had been virtually untouched by terrorism.

The record of the U.S. Intelligence Community changing in response to the threat from international terrorism goes back farther than the end of the Cold War and back before the episodes, the cases that were examined by your staff, back to the 1980s, when the main U.S. concern was with Hizbollah's activities in Lebanon, including the bombing of the embassy and the Marine barracks and the years of hostage-taking, as well as the terrorist activities of certain states.

The Community's principal response at that time, and in many ways still its most important response, was the creation of the DCI Counterterrorist Center or CTC, as it's called in 1986. This step was a bureaucratic revolution. It involved slicing across long-standing lines on the organization chart, bringing analysts and operators to work more closely together than they ever had before, and benefiting from the synergy that comes from having people with different skills and specialties attacking the same high priority problem together.

Further refinements were made in CTC in subsequent years. One for which I am proud to claim personal credit was the creation of a permanent cadre of counterterrorist analysts, replacing an earlier system in which the analysts working on counterterrorism were on loan from other offices which continued to control their promotions and their careers.

There were also reconfigurations within the Center, including the special bin Ladin unit which you've already heard about from Ms. Hill and others. Another refinement in CTC was the increased representation of agencies other than CIA, particularly but not exclusively law enforcement agencies such as the FBI. Much has been written and said particularly over the past year about the FBI–CIA relationship.

I find elements of truth in much of this commentary, but I also find most of it was dated. The relationship, although it had problems at the beginning of the 1990s, improved substantially during the course of the decade. This was partly due to a commitment at the top of each agency to make it work. And Director Freeh and Director Tenet both deserve a lot of credit for that. I would also add that the relationship with the southern district of New York, Ms. White's old office, became, as she already noted in her testimony, particularly close on the bin Ladin-related cases.

Along with these changes involving personnel and organizations, CTC's methods and operational strategy also evolved. Efforts to recruit well-placed unilateral sources continue to have high priority, but CTC developed during the 1990s a strategy that recognized that although information about specific terrorist plots was rare, other information about suspected terrorists and their activities was more feasible to acquire. The strategy was to work with many foreign government partners, foreign police intelligence and security services to disrupt terrorist cells using whatever information we could collect about them.

Most terrorists commit other illegal activity besides terrorism. And this became the basis for numerous arrests, interrogations and

other disruption initiatives, some of which my co-panelists already referred to as somewhat akin to nailing Al Capone for tax evasion. This type of disruption work must continue, in my judgment, to be a major part of major counterterrorist efforts. It is slow, it is incremental, it does not yield spectacular highly visible successes, but I am convinced that by impeding the operations of terrorists it has prevented some attacks and saved some lives.

The main lesson I hope the committees draw from this capsule history is there already has been a long and substantial evolution of the Intelligence Committee's approach to tackling international terrorism. Most of the innovations worth trying have already been tried. I'm sure all of us in this room wish there were some one further change or set of changes that would give us assurance that something like September 11 would never happen again. But I am not aware of such a step that would provide that kind of assurance, and I don't believe there is one even though there clearly is room and need for additional improvement as long as our counterterrorist batting average is anything less than 1,000, which means indefinitely.

As we work to avoid recurrence over the source of errors and omissions that have received so much attention in the September 11 case, we should try not to reinvent wheels already invented or, even worse, to undo beneficial adjustments made in the past. We should also be careful not to give the American people any sense that with some new set of changes the problem of international terrorism has somehow been solved.

Mr. Chairman, my written statement discusses other topics you asked me to address. But let me wrap up by attempting to respond to your request for recommendations. I'll mention a few matters that I think are of most direct concern to these committees, while emphasizing even major new efforts or initiatives are apt to yield only modest results. First, it is vital to have sustained, underscore the word "sustained," long-term public support for what the Intelligence Community needs to do in counterterrorism with everything that implies regarding resources.

The main impact that the various attacks on U.S. targets had on the work of the Counterterrorist Center over the past decade and a half was that those were the times when public interest in this subject spiked and resources went up. When public interest was lower as time passed without a major attack, which was the case as the '80s moved into the early '90s, resources were much tighter. The vital painstaking work of taking apart terrorist groups and terrorist infrastructures is long-term work. And it cannot be done with the kinds of ups and downs in support that have occurred some times in the past.

Second, we probably should try to make more extensive use of multiple sources of data including non-traditional sources to detect possible terrorist activity. By this I mean not just using watchlists and checking names while working on individual cases, although that is obviously very important, but rather a broader exploitation for intelligence purposes of such things as travel and immigration data and financial records.

I've always thought that trying to do this involved immense practical difficulties ranging from the use of multiple names to prob-

lems in getting some of the information from the private and public sources that own it. I still think it involves that. It would involve looking through huge haystacks with only a chance of finding a few needles. But the standards for return on investment in counterterrorism changed on 9/11, and perhaps this is an avenue that we need to explore further.

Third, and this goes far beyond what the Intelligence Community itself can accomplish, we must nurture foreign relationships to get the cooperation of foreign governments. That is so vital to a host of counterterrorist matters, especially including intelligence matters.

Of course, we need to continue to make every effort to develop unilateral intelligence sources on this topic. But in counterterrorism we will always be, for several geographic cultural and jurisdictional reasons, more dependent on our foreign partners than with just about any other intelligence topic I can think of. That is not a weakness. It is something to cultivate and exploit.

We need our foreign partners for information and we need them to carry out most of the arrests, the raids, the confiscations, the interrogations and the renditions that are involved in dismantling terrorist groups. This means that we need to give them the incentives to cooperate, and if necessary the assistance in developing the capabilities to do so.

Finally, we should take a broad view of counterterrorism and recognize that how much future terrorism occurs against U.S. interests will depend not only on what is done by people at the CIA or the FBI who have counterterrorism as part of their titles, counterterrorism involves not only learning the secrets of the next terrorist plot or erecting security measures around what we think is the next terrorist target, it also involves the motivations for groups to use terrorism and the conflicts and conditions that lead some people to join terrorist groups in the first place, even though there will always be some like bin Ladin who seem determined to do us harm, regardless of motives or conditions.

This broad view obviously gets into many foreign policy issues that go beyond the scope of this hearing. But the lesson for intelligence is that, as more priorities are given to particular counterterrorist accounts, we should not denude ourselves of coverage in other areas that not only are important in their own right but that also bear on possible future terrorism.

The Intelligence Community has an important responsibility not only to go after al-Qa'ida or whatever is the current predominant terrorist threat but to be aware early on of future or nascent terrorist threats, whatever form those threats might take and whatever ideologies they might espouse and what other conditions might lead such threats to emerge.

Thank you, Mr. Chairman. Those are my remarks.

Chairman GOSS. Thank you very much, Dr. Pillar.

We are now going to go to our normal procedure, minus Senator Rudman, of the designated questioners for today's hearing. For our witnesses' information, we've just basically assigned this to different members so that they're well prepared on the matters of the subject of the day. Representative Lahood is recognized for 18 minutes.

Mr. LAHOOD. Thank you, Mr. Chairman. I want to compliment both you and Senator Graham on the way you've conducted these hearings, and want to compliment our witnesses on the extraordinary amount of integrity and hard work that you have brought to your jobs of public service during the time that you served our country, and we thank you for that.

Judge Freeh, past hearings and interviews of FBI officials suggest that the Bureau, while missing many skilled and dedicated agents and analysts, was unable to coordinate activities against terrorism. In particular, the approach the Bureau used against organized crime, deadbeat dads, narcotic traffickers, did not translate well in its effort to fight a global enemy. Individual Bureau offices did not appear to coordinate their activities and headquarters often seemed unable to control them. In addition, the FBI's poor communication infrastructure made it difficult for FBI agents to communicate with each other, let alone with other parts of the Intelligence Community.

Judge, let me just see if I can put it in my own terms. After listening to a lot of testimony, there's a feeling, and I have this feeling, that there's a culture in the FBI, a culture that maybe dates back to Director Hoover all the way through your distinguished tenure as director, that offices don't communicate with one other, that agents within agencies don't communicate with another, that offices don't communicate with Washington D.C. or with higher-up officials, that there's a mindset, if you will, that takes place within the Bureau that says hold things close and don't be in touch with local law enforcement and don't be in touch with other offices.

And I have that feeling after listening to a lot of testimony as a member of this Joint Intelligence Committee. And so, with all due respect to you, sir, I'd like to hear your point of view. Is there a culture in the FBI that dates way, way back that trains agents in the idea that you can collect a lot of information but hold it close and don't share it?

And my concern is that the only way we change that culture, which I believe does exist, is when we recruit 1,000 new agents that the Congress has authorized and we train these people that this idea of holding things close is nonsense. It's not the way we do our job. So I appreciate the chance to have you respond to that kind of—I don't know if it's criticism, but an idea that's been purported around here. And I know you've read it and I know you've heard it and I want to give you a chance to respond to it this afternoon.

Judge FREEH. I appreciate that very much. To answer your question in two parts, with respect to information technology, again it was in the portion that I didn't read. The FBI, in terms of its IT infrastructure, its access and ability to use and capacity to do what private industries many other government agencies have done very well for a long time in organizing data, mining data, communicating data, we have a very inferior system. And I will take partial responsibility for that obviously being there the last eight years, although there's a story there that is pretty well set forth in my statement.

On the other issue, which I think is the more pertinent issue, I would respectfully disagree with that. I say that the notion that

the FBI, whether it's working in a counterterrorism matter or criminal matter, has a culture where information is not shared is incorrect. And I think it's dated. It's much like the notion that the FBI and the CIA don't speak to each other.

This committee, I think better than any other committee, knows that that's incorrect. There may be a perception out there that the two agencies did not speak to each other. As Mr. Pillar mentioned, maybe that was true, ironically, during the Cold War when we should have been speaking to each other more, but that is not the case anymore.

The notion that we have a culture that withholds information from our State and local partners is absolutely incorrect. And I would encourage you to speak to the President of the International Association of Chiefs of Police. We didn't have 34 joint terrorism task forces throughout the United States because the FBI is not in the business of working with and sharing information with our State and local partners. The Joint Terrorism Task Force in New York dates back to 1980. It's the template of how the FBI, which at one time in its history—which is why I characterize the perception as dated—did not share information and in many cases was guilty of monopolizing information and not sharing it.

But that is, as I say, 20-year-old perception which is not true. You can talk to police chiefs around the country and, maybe more demonstrably, police chiefs around the world. The FBI has a culture and a protocol and a very well-established tradition now with respect to sharing information. And I would encourage you to speak to mayors and chiefs of police and whatnot.

Now, going back——

Mr. LAHOOD. With all due respect, Judge, I have talked to local law enforcement people. And they have told me that there is a disconnect between local offices. I agree with you that if you use the southern district of New York blueprint, the Rahman blueprint, if you will, where a lot of information was shared, you do get the prosecutions and there's a lot of information shared, but how do you explain the Arizona memo? How do you explain the idea that there was information out there that never reached the highest levels of our government? How do you explain that other than people weren't communicating with one another?

Judge FREEH. You're absolutely right. In those particular instances, there was a lack of communication. But you're talking about a culture and generational gap and hiring new people that understand sharing information. My response to that is that is ignoring what I think is the routine and the operational capability and history of our agency. We are not an agency, have not been for the last decade, that is in the business of monopolizing and securing information that is routinely disseminated and used by our State and local partners.

We have dozens and dozens of safe street task forces around the country; maybe you should ask some of your mayors and police chiefs about that. Every major city has a safe street FBI task force, nothing to do with terrorism. They work cold homicides, they work hijacking cases, and they work with State, local and FBI agents in the same space under the same leadership.

So what I'm telling you is that there is—there is an absolute misperception if there is a notion that we have a culture where information was not shared. That wasn't my experience in eight years. It was my experience in 1975 when I was a new agent reporting to the New York City FBI office and I was told I wasn't allowed to work with the New York Police Department, which is pretty hard when there's 30,000 of them in the city. But that is a very dated concept and one which is not the reality today.

Mr. LAHOOD. With all due respect I would say this: I know that there's communication, I know there's project exile task force and other task forces, but on the issue of terrorism, on the issue of people that are in our country illegally and that are here to do harm to our country, I'm not sure that what you're saying really holds true for that aspect of people who are here illegally and want to do that in the United States. I don't think it's been true. And I don't lay all the blame at the Bureau, but certainly Immigration and Naturalization and others probably share responsibility.

But when it comes to terrorism and fighting terrorism, with all due respect, Judge, I think there is a disconnect and there was a disconnect. And I've been told by Director Mueller that he's correcting that. And I can't say that you and Director Tenet didn't communicate. I'm sure you did. I'm sure you had meetings. And I know that Director Mueller and Director Tenet are meeting on a regular basis now. My point is that there's a feeling out there that this wasn't happening within the agency, between offices.

Let me just see if I can ask another question because my——

Judge FREEH. If I could just respond to that, because I think it's very important, and I again commend the chairman for having a public hearing and for you asking this question. You just gave an example which I'll respond to. You talked about meetings and communications between the Directors, the FBI Director and the DCI, about the agencies not communicating.

You have to know from your briefings, because I did the briefings myself here, there was a long history over the last several years where CIA officers and FBI agents together went around the world exploiting Hizbollah cells, al-Qa'ida cells, the agent being present so chains of custody be maintained so Mary Jo White's prosecutors could use the evidence and the Agency's officers present for covert intelligence. You can't understand that reality and defend or support a misperception that these agencies——

Mr. LAHOOD. How do you explain the Arizona memo then, Judge?

Judge FREEH. We can take a single bit of information, we can take the Phoenix memo, we can take other pieces of information. I'm not saying there weren't gaps or disconnects, I'm not saying that information about two of the hijackers in 2000 didn't make the intersection that it should have made, but, you know, we can talk about the particulars or we can talk about the reality of how things are actually being done. And I think it's instructive to talk about both, but not one in isolation to the other.

Mr. LAHOOD. Well, let me—you and I disagree on this, and I think we've heard an awful lot of information. And going back to what I said, if you use the Southern New York District blueprint, it's a good blueprint, because I think a lot of communication took

place, notwithstanding all the obstacles that the former U.S. Attorney mentioned, and I think there have been task forces on some issues, but not on terrorism in this country.

I'm sure there are people that traveled all over the world and tried to find terrorist groups. But I'm not sure that was happening here, and I'm not sure that the communication was really going on here. And I do think this needs to change. Director Tenet declared in December 1998 that we are at war with Usama bin Ladin. Was the FBI on war footing with al-Qa'ida prior to September 11, 2001?

Judge FREEH. Absolutely. In 1999, not only had we indicted Usama bin Ladin twice, he was on our top 10 list; al-Qa'ida was the number one priority. We had a dedicated unit. We had an Alec station that was set up with the CIA to work exclusively on those cases. We were indicting people, we were bringing them back to the United States, we were convicting them. We were exploiting intelligence with the Agency officers all over the world. There's no question in my mind that that was a number one priority.

Mr. LAHOOD. Ms. White, do you agree at all with my notion that I have stipulated here about the idea that there is a culture within law enforcement at the highest levels not to share—I know it didn't happen in the southern district, I know that. But you've been around and you've—I'm just curious what your idea about this is.

Ms. WHITE. No, I essentially agree with Director Freeh about that. I think that again 25 years ago that certainly that was true, I think particularly between Federal agencies generally and local agencies, police departments generally, and some of your more veteran police officers kind of hearkened back to that.

One thing that happened in New York, where I think the relationships are extraordinary between the FBI and the local authorities, but once 9/11 happened, even there where the communication was excellent, the conclusion was reached, the erroneous conclusion, was there must have been something not shared. You heard that everywhere. And my response to that in talking to the police officers was, you know, was that there was something to have shared. I mean, it wasn't an absence of sharing.

So I think I do agree with that. I think there is—my own perception if there's a communication barrier, and that doesn't just apply to the FBI, and it's not cultural really, but one must do better, I think all the agencies between the field and headquarters. I mean, I think there are some barriers there. There are also some barriers built in by what I talked about this morning by the intelligence side and the law enforcement officer side.

But I think a lot of the perceptions particularly in the local agencies is really a dated one as Director Freeh says.

Mr. LAHOOD. I will just tell you this, Judge and Ms. White, we went to New York as a part of a subcommittee, and we heard testimony from the police commissioner and the mayor there, Mayor Giuliani, when he was mayor, and also this committee has heard from the Chief of Police of Baltimore, and it's not really in sync with what you're saying. I wouldn't be raising this issue if it hadn't been raised here. I'm not trying to raise it to embarrass anyone.

I'm not trying to raise it to embarrass you, because you have a distinguished record, Judge. But I do think there's a feeling out there that the culture has to change, that information does have

to be shared and that perhaps it wasn't—on the terrorism stuff, not on some of these other issues. I know there are task forces on drugs, on exile. I know that the offices are working closely with the local police departments on these things.

My son is an assistant U.S. Attorney in Las Vegas. He's on a task force that works with the local police on rounding up people who use guns illegally. But I'm talking on the terrorism stuff and during the time that you were Director. So obviously we have a disagreement on this. And so I guess we'll have to—what was the process by which supervisors and special agents in charge were held accountable for adhering to investigative priorities set forth by headquarters?

Judge FREEH. Well, we have an inspection process which is separate and apart from the administration of the individual program such as terrorism and organized crime and white collar crime. Each of our offices, 56 main divisions, are inspected, usually about once a year every 18 months. And a team of those inspectors who come from a non-operational division review the implementation of the strategic plan with respect to all the component programs. And if a plan is not being performed in the office, if the U.S. Attorney is complaining, if our State and local partners, who are all interviewed during the inspection, raise the very issues that you've raised with me, we take action against whoever needs to be acted against, whether it be a supervisor or a program manager or an SAC.

Separate and apart from the inspection process, there is the individual program management. Dale Watson, who you know, who has testified here, was responsible for the counterterrorism programs and had individual supervisors in the 56 officers who are accountable to him for the administration of the plan, the working of cases and all the other implementation.

So it's sort of a dual process. And over and above that, of course, is the Department of Justice review, Inspector General reviews, oversight by the committee, budgetary reviews, and other layers.

Mr. LAHOOD. Do special agents in the field enjoy too much autonomy?

Judge FREEH. Not in my view, they don't. In fact, they're accountable every day not only to their supervisors, but one of the benefits of a law enforcement agency in a democracy is they are accountable to courts, to judges, to juries, to defense attorneys, to the media. They have absolute transparency particularly as a case is developed and moved along in the trial process, which is one of the strengths of our agency, that you know we have this accountability.

It also means that our mistakes are always public, which is actually a good thing for an agency with the power of the FBI.

Mr. LAHOOD. I would like each of you to comment, if you would, on the notion of a blue ribbon commission to look into what happened on 9/11 and to make recommendations, if you would, please. This is my last question, because the yellow light is on. But I would appreciate any comments. If you don't feel compelled, I understand. But I know that each of you have been involved in these matters, and if each of you would comment and if you'd like to go first, Mr. Pillar, and then Judge Freeh, and then Ms. White. Thank you very much for being here, too.

Dr. PILLAR. I would welcome the thought of a blue ribbon commission, simply because the whole problem of counterterrorism goes far beyond intelligence or even beyond intelligence and law enforcement. And there are a host of other things that get into foreign policy, national allocation of resources that I think a commission with a broad view would be appropriately equipped to address.

Judge FREEH. Yeah, I would agree with that. I think Senator Rudman's remarks and obviously some of the questions and commentary about the organization of the congressional committees with respect to oversight is an important issue and that's probably better looked at, at least in the first go-round, by an independent commission.

Ms. WHITE. I would strongly favor an independent commission and one that's permanent, frankly. I think this subject of international terrorism and Homeland Security is not only the most vital subject that we have, but one that's extraordinarily complicated that I think can't be done in the short run. I think there should be one. I think there should be a permanent independent commission.

Mr. LAHOOD. Thank you very much. Thank you, Mr. Chairman.

Chairman GOSS. Senator Feinstein.

Senator FEINSTEIN. Thanks, Mr. Chairman.

Director Freeh, I just want to thank you for your service to the FBI and to the country and you certainly made a very precise and spirited defense of the agency, and I know there are a lot of people that appreciate it.

Ms. White, I want to thank you for your service. I think you've run one of the foremost U.S. Attorney's offices, or did run, in the country and thank you for those very successful prosecutions. And Mr. Pillar, I just want to say that your views for me are having greatly increased value. The more I listen to you, the more I see the depths of your knowledge. So I thought it might be a nice thing to say that.

Ms. White, let me begin with you on FISA, because it's been a kind of ongoing interest for me. And that subject is the wall. As you know, we're still awaiting an appellate decision from the FISA court. But in the PATRIOT Act, we changed the standard for FISA from a primary purpose must be foreign intelligence, and added the word "significant purpose."

And now the recommendation of the Attorney General is essentially to even break that down further. What are your views? Do you believe that "significant purpose" is substantial enough to overcome and break down as you describe that wall to be?

Ms. WHITE. I would have thought so until the FISA court decision. In fact, as I think I mentioned this morning, I was instrumental in making the recommendations in both directions to get the walls down, and I think there's no question that the "primary purpose" test, which I guess was engrafted actually by courts prior to the USA PATRIOT Act, to some extent did retard, I think, seeking FISA applications out of a concern to defend, you know, that record, that indeed if there was a criminal prosecution and you had to defend the FISA wire that you want to be very careful and very conservative about that. I think too conservative. I think the Justice Department was too conservative in some ways. But there's no

question that the "primary purpose" test was a cause of a lot of that. I would have thought the change to a "significant purpose" would have been sufficient, but I doubt that now given the decision.

Senator FEINSTEIN. Well, this is another day, but I would certainly, if you have a recommendation there, we may revisit this subject in the future—I'd certainly——

Ms. WHITE. I'd be happy to give it to you.

Senator FEINSTEIN. Very much like to have it.

Mr. Freeh, if I might, in reading through Dr. Hoffman's written report here—he's Vice President of the Rand Corporation—he points out, and this was interesting, that really not until 1980, as a result of repercussions from the revolution in Iran, did the first modern religious terrorist groups appear. And that amounted that year to two of 64 groups that were active during the year. Twelve years later, the number of religious terrorist groups had increased nearly six-fold, representing a quarter of the terrorist organizations who carried out attacks in 1992.

Significantly, he says this trend has not only continued, but it has accelerated. By 1994, a third of the 49 identifiable terrorist groups could be classified as religious in character and motivation. In '95 their number increased yet again to account for nearly one-half of the 56 known terrorist groups active that year. And then he points out the higher levels of lethality of religious terrorism.

Now, my question ties in with that, because I think for a law enforcement agency that even makes the intelligence-gathering much more difficult. Agents that I have talked to when I have had a chance to sort of talk to them informally have said that most of their work surrounds the opening of a case rather than pure intelligence-gathering. If you add to that the religious overtones of this, it seems to me it makes the gathering of intelligence, its dissemination, its collection and dissemination to a variety of sources even more difficult.

And if you lay over that the sort of the culture of the FBI, which is primarily law enforcement, how then can you really carry out where we have to go, which surrounds religious fundamentalism that has lent itself to the very lethal terrorism? How do you collect that from a law enforcement agency subject to the law and the strictures that an FBI agent is subject to?

Judge FREEH. It's an excellent question. I don't think it's so much a culture of the FBI or the complexity of the task, admittedly, which is the obstacle. I think it's a combination of resources, legal authorities. You've discussed some with Mary Jo White. You know, the FBI for decades was very effective, I think extremely effective, in working counterintelligence matters during the Cold War, during World War II when there wasn't a CIA. The FBI was stationed, as you know, all over the world, in South America, performing the collection and disruption functions that the Agency took over when the National Security Act of 1947 was passed.

So I think although we're a law enforcement agency we have a very long tradition. You heard Senator Rudman this morning. The collection ability is there and it shouldn't be displaced to some new entity without the history or transparency when it's necessary that the FBI has it in that regard. But your question and Professor Hoffman's point is an excellent one. The complexity here is over-

whelming. I think that's one of the misunderstandings of al-Qa'ida, not in this committee but around the world.

Al-Qa'ida is a facilitator. It's not just an organization. The people who trained in the al-Qa'ida camps or trained in the al-Qa'ida camps in Afghanistan, like Ressam who was not an al-Qa'ida member but was trained by them, will tell you that the class that was reporting that week for training became a cell facilitated by a global al-Qa'ida network but not an al-Qa'ida organization per se. Which is why when you say that you know there's a—there's not a focus on the al-Qa'ida organization, well, the al-Qa'ida organization is potentially 10,000 to 25,000 Afghan war veterans who are all over the world.

So, I think in response to your question the complexity here is enormous but it's not beyond the capacity of resources and focus and legal authority to address. But it certainly can't be addressed with the current resources.

Senator FEINSTEIN. In your written remarks and your verbal remarks you say that the direct evidence obtained strongly indicated that the '96 bombing, this is Khobar, was funded and directed by senior officials of the government of Iran. The Ministry of Intelligence and Security and Iranian Revolutionary Guard Corp were shown to be culpable for carrying out the operation.

The bombers were trained by Iranians in the Bekaa Valley. Unfortunately the indicted subjects who were not in custody remain fugitives, some of whom are believed to be in Iran.

Also read the New Yorker article. Now, this places us in a very unique situation with respect to the debate that's currently going on over Iraq. Here is a direct government connection to a terrorist attack that our premiere law enforcement agency has discovered. To whom did you relay this information and what did you ask to do about—I mean, what did you ask them or say to them, that you wanted to do to carry out arrests or activities, or what advice did you provide?

Judge FREEH. Well, first of all, that information, as we received it, which was the product of interviews, direct interviews by FBI agents, was immediately reported to the Attorney General, the National Security Advisor, this committee. I think it was a few days after that briefing when I came here and to the chairman and the vice chairman, in very secure fashion, gave them that exact information.

With respect to what I asked for or recommended, the only objective that I had, because my instruction was to make that case and work that case and leave no stone unturned, which is what I tried to do, was to identify and indict and then have apprehended any and all people who were responsible for that bombing. So that was my objective and that was my recommendation.

Senator FEINSTEIN. And just leave it at that, take no other stronger actions with respect to Iran?

Judge FREEH. No, I would not have made that recommendation. That's not the place of the FBI director or nor was that our tasking. Our task was to work the case, find the evidence, indict who could be indicted, and find who could be found, and that's what we did.

Senator FEINSTEIN. In the New Yorker article, a conflict was related between you and the administration over the bombing. Did you, in fact, believe that you didn't get the support you needed?

Judge FREEH. Well, we got an indictment, and we got there after five years. We got there by a lot of hard work, by developing relationships, by making requests for assistance which ultimately were granted. Was it a perfect scenario? Was it one conducted without frustration? No. But I measure the success of which was the indictment that was returned.

Senator FEINSTEIN. The Inspector General, in a recently-released audit of the FBI's counterterrorism program, pointed out that the FBI never provided a comprehensive written report on the training, the skill level, the likelihood of attack or other basic characteristics of the terrorist threat to the United States. Why was that?

Judge FREEH. Well, my understanding is that there was a draft threat assessment which was done before September 11. We also participated in a five-year study and recommendation which the Attorney General had organized. The threat assessment apparently was not as specific as the GAO inspectors wanted it, but there was, as I understand it, a draft threat assessment which was completed before September 11.

Senator FEINSTEIN. Is that available to us? Well, I'm sure it is.

Judge FREEH. I guess I'm the wrong person to ask.

Senator FEINSTEIN. Be interesting to find out.

Judge FREEH. I think that's noted in the GAO report actually.

Senator FEINSTEIN. Okay. After DCI Tenet, whom you commend, and of course we do as well, declared war on al-Qa'ida in December 1998, at any time after that did the White House or anyone inform you that al-Qa'ida was a Tier Zero target?

Judge FREEH. No, I mean not that I recall. But everybody in the White House, and certainly everybody in the FBI, by December of 1998, had focused on al-Qa'ida as the primary target. That terminology that you use Senator, I apologize, I don't recognize it. It was our number one priority. By the time DCI Tenet declared war, Mary Jo White had already indicted bin Ladin two times. There was no question in anybody's mind working that program that he and al-Qa'ida were the number one priority.

Senator FEINSTEIN. You have some recommendations in your written report. Based on your rather considerable experience with these terrorist bombings, in terms of turning the FBI—not turning it but encouraging its intelligence gathering, and the communication of intelligence, its dissemination, to other intelligence agencies, what do you believe is the single most important thing that could be done? Because the comments that we receive is that the FBI doesn't turn over intelligence. We've heard that, at least I have, from the NSA, we've heard it from the CIA. Other than putting detailees, which has been the case, to work in the CTC, which is one way of doing it, how do you break down—I don't want to use the word culture, but that's the word that's been used to define, what's the single most important thing that you would recommend be done?

Judge FREEH. Okay. I think there's a couple things. And I don't subscribe to the characterization of culture. It's a generality to me that doesn't have any relevance. But I think you do it a number

of ways. You do it by a top-down decision and implementation of the kinds of sharing initiatives and motivations and opportunities that existed. We brought a succession of senior CIA officers, as you know, over to the FBI and senior FBI agents went over to run the Counterterrorism Center as a deputy on numerous occasions.

The notion there was a simple one, that not only would we have an exchange of officers, but the CIA officers who came to the Bureau had line authority in the counterterrorism unit. That's one way.

The other way I recommended in my recommendations was interoperable databases. We don't have that—not just between the FBI and CIA, but around the government. It is a hugely expensive but not technically complex solution to most of the problems that we've been talking about and that you've been hearing about in this committee—gaps and lapses in little facts, and bits of information going where they need to go quickly and efficiently. We don't have that.

Obviously resources, statutory authority. The PATRIOT Act goes a long way in breaking down the wall that you and Ms. White were talking about a moment ago—you know, changing the domestic guidelines and the FCI guidelines, which are now being changed, by which the agents in the field have operated for many, many years with respect to opening investigations, using sensitive techniques et cetera, et cetera. So I don't think there's one single thing, although the interoperability of data which almost guarantees participation and exchange because of the momentum of that technology would really be critical.

Senator FEINSTEIN. Even encryption, which is something that I was interested in, and I recall that you met in my office with some of the CEOs of the major computer firms on this issue. I was under the impression that agreements had been worked out with respect to the key issue, and that the problem was somewhat solved. Is that the case today, or is it not the case?

Judge FREEH. No, that is not the case. And I would give you more credit than just participating in the meeting. You set the meeting up with the senior CEOs in the industry and pursued that. We have, right now, some very important and very successful voluntary arrangements and exchanges with industry, which go a long way to solving the problem. The problem, however, is not solved. There is absolutely no legal authority for your law enforcement officers to retrieve without a court order in hand the plain text of a terrorist or someone else in an intercepted communication or in some stored data. They fixed it in the U.K. The parliament passed the statute. We tried here as you know, many, many years.

Chairman Goss, I can't praise you enough for your leadership and your industry, and Norm Dicks, who's not here. We got absolutely no support any place in the government, quite frankly, either down the street or up here. It is the single greatest vulnerability to our technical capacity to prevent terrorism. And it is unaddressed in the PATRIOT Act. It is not being addressed any place else. It is mind boggling that with the political atmosphere and the momentum we have to fight this war that we cant fix this.

Senator FEINSTEIN. My time is up. Thank you, Mr. Freeh. Thank you.

Chairman GOSS. Thank you.

Mr. Roemer.

Mr. ROEMER. Thank you, Mr. Chairman. I want to just thank you and Senator Graham and the ranking members of this committee for your leadership and your long hours of work to lead this committee, I think, in a proper and helpful direction to better understand not only what happened on September 11, the horror of that event, but also to try to better understand back through the previous seven or eight or nine years, starting with the bombing in 1993 of the World Trade Center, what kind of enemy we're up against, what kind of successes we've had, and certainly the people at this table have had considerable successes but also, I think, what kind of mistakes or failures or disconnects or gaps are in the system and still existing in the system so that we can go forward and fix the problems.

I'm hopeful that these hearings are not about fingerpointing and blame games and seeking to pin the tail on somebody, or even, as Judge Freeh talked about, a smoking gun. I think we're talking more about what kinds of mistakes and gaps and cracks are in this system that allowed these snakes to crawl through and attack our people, inflict incredible damage and kill over 3,000 people.

Ms. White, I'd like to start with you because of some of the things I've read about your successes. You dusted off a 140-year-old law that hadn't been used since the Civil War to go after terrorists. You took a very creative approach. You called it, or it was called the Law of Seditious Conspiracy to go after enemies of the United States and to increase penalties from 5 to 20 and 30 years, if you could successfully prosecute them. You also said in your testimony that you realized in 1993 you were up against, and I'll quote, a long term, "highly dangerous enemy."

It wasn't something that was a freak accident in 1993. You then sought to share with other Federal law enforcement agencies the Intelligence Community information. But beyond sharing I think we are talking about true collaboration and implementation. I'm tired of hearing the word "sharing." Sharing too oftentimes around here means you bucked it over to somebody else and nothing was done with it.

So I would like to know, fairly succinctly, if you can to get the conversation started, what kinds of formal mechanisms and informal mechanisms did you put in place to get this cooperation to work successfully on these series of questions through the 1990s to prosecute, but also to look back, to compile this information on al-Qa-ida and to start to put together the pieces that we knew we were in for a long fight and to try to help make us preventive rather than reactive.

Ms. WHITE. To some extent it happened initially by happenstance. The Trade Center was bombed in 1993 in our district. As I think I said in my testimony—it is in my written statement—because of the Day of Terror plot, which really was at the same time, but I call it the follow-on plot, and what we learned from that, that is what convinced me and others in my office working on these matters and the FBI obviously, it is long-term, it's a dangerous risk.

From there, we did make the decision that we didn't want to lose that information. We knew what we didn't know, too. We didn't know nearly as much as there was to know. We knew the risk was there, we knew the danger was high. And then we proceeded in a terrific working relationship with the FBI and the CIA throughout the years, eventually culminating in the joint efforts of the Bureau and the CIA on bin Ladin and al-Qa-ida that we have all talked about, culminating in his indictment by our office before he attacked anyone in June of 1998.

But it's a long-term process. You learn more every day. To me the key is getting the information in one spot where—not one spot, but in an integrated place at least where it is understood and can be acted upon.

One barrier that I didn't mention I would like to, and then I'll be quiet here, is the difficulty of language in dealing with terrorism. I know you've heard a lot about that and there aren't enough interpreters. That is a huge, huge problem. You can have every FISA application in the world approved but if you don't know what your reel of tape says, and we ran into that——

Mr. ROEMER. Or translating the evidence?

Ms. WHITE. And it is not just Arabic but it is an obscure dialect of Urdu or Arabic and there aren't many people in the world, certainly with a security clearance, that can understand accurately what you have. So to me, going forward, the more we can do to understand what we have real-time and then share it real-time, but we are a long way from that.

Mr. ROEMER. I appreciate your comments about language. We're trying to work on that very area in our intelligence authorization bill.

Ms. White, you must have at times—as the Blind Shaykh case and the Manila plot and the bombing of the embassies, as all these things are coming down on you, did you ever say you're overwhelmed? Even though you thought you had pretty good communications set up with other agencies, did you ever say, we're not going to get it done this way, we need more cooperation with the intelligence, we need military help to go after the sanctuaries, this is not going to do the trick, we've got to take this higher?

Ms. WHITE. The cases, we got extraordinary cooperation on. They were exceedingly difficult. I think the success rate masks how difficult they were, but the cooperation we got from the Bureau and the Intelligence Community was extraordinary. But again, as you've heard us say this morning, and certainly it was my view, when we could act to neutralize we did, through criminal prosecutions and investigations, but this was a much bigger problem. This in my mind very early on was a problem for the military. We're talking about a worldwide——

Mr. ROEMER. Did you ever bring that up? Did you ever go to anybody and say I'm overwhelmed, we're not going to get this done through prosecuting cases, we're not going to even get this done through good collaboration, this is a lot bigger for this district and for the country than this?

Ms. WHITE. Again overwhelmed, not overwhelmed in the cases, as difficult as they were. But I certainly expressed the view to the officials in the Justice Department. Director Freeh and I discussed

it. This was quite clear, but again I go back to what I said this morning. I was not under the impression that prosecutions were our counterterrorism strategy. I still am not. Even from my vantage point there were a lot of other things going on—not the military effort obviously we had after September 11, which I would have liked to have seen as a personal matter after the East Africa embassy bombings.

Mr. ROEMER. When you, Ms. White, would press this and be concerned to other people, whether it was Director Freeh at the time or whether it was somebody in Justice, did they ever get back to you and say we brought it up with such and such and we received a good response or a poor response on that?

Ms. WHITE. Again I think the response was, everything's under discussion. And I did think our government——

Mr. ROEMER. Including military?

Ms. WHITE. Under discussion. But again I know what I know and I don't know what I don't know. I didn't interface with the Department of Defense or the White House or the NSA. I interfaced with the Attorney General and Director Freeh, Director Tenet from time to time. That's as high as my pay grade went in a sense. But, even from that vantage point, it was definitely my impression that our government as a whole was taking this threat very seriously and thinking comprehensively about what to do about it other than by way of prosecutions. But I was not in that direct loop.

Mr. ROEMER. And isn't there a sense of frustration and irony that with all this work, with one of the most effective collaborative efforts we have in the Southern District, that they come back to New York and successfully strike again?

Ms. WHITE. I think coming back to New York, as horrible as that was and would have ever been, was not something that we didn't expect to happen. The Trade Center was obviously, it was a symbol of our economy, our capitalist economy. Al-Qa'ida particularly is into symbolic targets of our system. New York and Washington obviously are right up on that list and always have been. So as tragic and horrific as it was, and it was and it is, it did not come as a surprise that they came back to New York. I think all of us thought it was a matter, whether it be New York or somewhere else, but certainly including New York, there was going to be another attack.

Mr. ROEMER. You were not surprised that they came back?

Ms. WHITE. No.

Mr. ROEMER. Judge Freeh, let me read to you testimony from a House subcommittee of yours in 1995. Everybody says when George Tenet declared war on al-Qa'ida in 1998. You said this as far back as 1995. "I'm greatly concerned about terrorist attacks here on American soil. The effort, as in Oklahoma City, will be to murder as many as possible through a single blow." Is that accurate? Is that your quote?

Judge FREEH. Yes.

Mr. ROEMER. So back in 1995, six years before they successfully come after the World Trade Center for the second time, you are predicting that they will do this. After the 1998 Africa embassy bombings, there are some 200 FBI counterterrorism cases that are opened after that bombing. Can you quickly tell me how do you

communicate with and follow up on these kinds of domestic cases? Not overseas; we know you did your best on the Khobar and you followed through on some of these things. What are you thinking and what are you trying to pursue domestically then in that case in this particular specific area?

Judge FREEH. I'm pleased to answer the question, on two levels. One, the 1995 statement speaks for itself. But, of course, that is, as you have heard here several times repeated today, that is a description of the 1993 World Trade Tower bombing where the plan was to, as mentioned by my colleague here, destroy two towers. In fact, Yousef told us after the event that they also wanted to lace the fertilizer bomb with chemical weapons so they could kill thousands but didn't have enough money to complete the plan.

But that brings me back to my early point. We were intensely focused on the domestic threat here in the United States, and the notion that we were fighting terrorism overseas and consumed overseas is absolutely inconsistent with our experience and that reality.

Now, the 200 cases. Cases are opened upon leads, credible information, whether they come from informants or electronic surveillance. If you notice, hundreds and hundreds of cases are being opened in the United States on the basis of information and leads which have been exploited in Afghanistan, a very important source of leads with respect to potential terrorists inside the United States. That is where those cases generated from. How are they monitored? Like any other case that we are responsible for which is of significance.

Cases come in different forms. In July of 2000, we indicted a group of people in Charlotte, North Carolina. You may not have noticed the press release because they were being charged with cigarette smuggling. But they were radical Islamic fundamentalists whom we believed were terrorists and we couldn't make a terrorist case on them, but we could make a cigarette smuggling case on them. So the cases are worked like any other case, but you need leads to generate them. You need credible information, even uncorroborated, to start that process. The explosion of cases that you see now, many of them are because FBI agents in Pakistan and Afghanistan, working with their colleagues, are finding hard drives and images which are leading to identification of terrorists within the United States.

Mr. ROEMER. Judge, as hardworking as you are, as prescient as you were, saying this is going to happen as far back as 1995, and as honest as you are, I admire you personally and professionally. But don't you feel at some point with all this going on in the world and your frustration in communicating—you have just talked about how frustrating your technology was, with 56 field offices—how do you follow up, with that kind of 20 or 30-year-old technology and communication systems, with 200 counterterrorism cases that are open in the field? This has to be extremely frustrating for you at the top of this pyramid.

Judge FREEH. Extremely frustrating. As I said in my opening statement, we are on our way to fix that and it is not rocket science. It's desktops, it's servers, it's networks, things for the most part you can buy off the shelf and then maybe modify for security

reasons. We didn't have that technology. We tried to get it. As I said before, I take responsibility for not getting it all when we needed it most.

Mr. ROEMER. Is it getting there now?

Judge FREEH. Trilogy now has been funded for part 2 and since September 11 the Congress has given several hundreds of millions of dollars for this technology. So we're well on our way to doing that. Could we have used it before? Absolutely. Could we better work the 200 cases? No question about it. We worked cases for the last 94 years. When I was an agent I used to keep my data on an index card. We could still work the cases, but you can't deal with a global organization that uses the Internet and hawala-financed transactions and has, as I mentioned before, not an organization but a pan-national collaborative membership with index cards.

Mr. ROEMER. But if your field agents are working off index cards and not collaborating and sharing information through a database about information collected in Phoenix or Oklahoma City or Minneapolis with respect to people from the Middle East training in schools for pilots, you cannot run a modern system with that kind of antiquated communications, right?

Judge FREEH. No, it cannot be done.

Mr. ROEMER. So how could we have done this, how could we have coordinated these counterterrorism cases at this point with this kind of old system, index cards and legal files sitting in a file case back in the office in Phoenix?

Judge FREEH. The fact of the matter is, we made some extraordinary cases—as Ms. White mentioned—prevented major acts of terrorism in 1993 when we had maybe not as antiquated a system vis-a-vis 2001 but still a subpar and not state-of-the-art system. I'm not saying we couldn't make any cases, in answer to your question about the 200 cases. We could do them better and we could coordinate all these bits and pieces much better than we have done with better technology.

Mr. ROEMER. You have said a couple of times that you had an excellent relationship with Director Tenet. To what extent, Judge, was your work with an agency such as the NSA to pinpoint sources of communication in the U.S. which were directed at known radicals abroad? Did you have a good relationship with General Minihan and then General Hayden? How often did you meet with them? Did you work with the NSA to go after known radicals?

Judge FREEH. We had personal, excellent relationships. We had agency relationships. They were present in the Counterterrorism Center, not just at the Agency but at the FBI. There were exchanges of information, not the exchange of officers to the extent that there was with the CIA, but their dissemination to us under whatever circumstances they could disseminate was clearly not as expansive as the flow of information coming from the Agency. But we had good personal relationships at the top. I think they will confirm that. And we had agency relationships, although not as extensive as the ones with the CIA.

Mr. ROEMER. How do we try to improve as quickly as we can the relationship between the FBI and the CIA, not with information-sharing, not with sitting down in a meeting and simply talking to one another but the collaboration, the follow-up, the implementa-

tion? How would you suggest that; given that you say you had a good relationship with the current Director, what would be your two or three pieces of advice to Mr. Tenet and Mr. Mueller to get that relationship off to a very good start? And how do we improve that in future?

Judge FREEH. I think the interoperability of our data is probably critical. As I alluded to before, having that infrastructure dynamic would actually start driving some of the personal relationships because the data would be transparent and readily exchangeable and viewable. That's the first thing.

The interoperability of our agents and officers overseas, for the first time in the history of the agencies, Mr. Tenet and I had our Legats meet with our station chiefs all over the world, overseas as well as back here in the United States. That was complemented by the officer exchange at headquarters that I mentioned. The cases that were worked in New York, again, we had dedicated FBI and CIA teams working overseas, exploiting information, conducting counterterrorism operations for intelligence purposes and simultaneously for obtaining evidence, maintaining chains of custody and using it in evidence.

That is the kind of collaboration that goes well beyond the two Directors sitting down and having an excellent relationship, which they did and do have at this time. Those would be my top three recommendations.

Mr. ROEMER. I want to thank the panel again for their work in the past on terrorism. Mr. Chairman, thank you for the time today.

Chairman GOSS. Thank you, Mr. Roemer.

Senator Roberts.

Senator ROBERTS. Thank you, Mr. Chairman. Inside the Joint Investigative Staff briefing book cover we find the topic of today's hearings; i.e., Lessons Learned, and I am talking about the 1993 World Trade Center, the 1996 bombing of the Khobar Towers, the 1998 attacks on our embassies, the 1999 planned attack during the Millennium, and the 2000 attack on the USS *Cole*. I think the attack on the USS *Cole* is really a microcosm of the challenges we face in regard to 9/11, and I am pleased to announce the Intelligence Committee's findings of a week ago in regards to our findings and recommendations in reference to the *Cole*.

Finding number 1: the Central Intelligence Agency, the National Security Agency aggressively collected and promptly disseminated raw intelligence pertaining to potential terrorist threats. Although the Intelligence Community analysts in Washington often had access to intelligence available on the global terrorist activities, they did not always enhance their products with historical information. As a result, field operators and analysts with limited resources to apply to historic research were often left with that task. The process was further hampered by limitations on intelligence-sharing.

There are a lot of changes, I'm paraphrasing here, in the Intelligence Community, but the lack of historical context for terrorist threat products and failure to abide by warning guidelines is a problem.

Finding 3. Intelligence available prior to the attack on the *Cole* was not provided to consumers in a final warning product prepared and issued by the Interagency Intelligence Committee on Ter-

rorism. We had some recommendations where we asked the DCI to report back to us basically with a detailed description of the steps the Intelligence Community is taking to increase the analytical depth on the terrorist targets; second, to revise the existing procedures and standards for issuing any formal Intelligence Committee warning products. That system should include a streamlined interagency and coordination process, clear and concise standards for issuing warnings, and a system of threat ratings for the consumer incorporating such factors as the immediacy, the significance and the reliability of the threat.

All the way through this, and the reason I went to the length of reading that is that we keep coming back to the bottom line in regards to the *Cole,* any of these lessons learned in this whole investigation, and that is the need for better analytical ability and a better predictive warning and analysis. Put another way, with all due respect to my colleagues, I don't think many of us have had an opportunity to meet or visit with or learn from a real, live, experienced regular analyst or understand what it is they really do. It is a lot like when you leave your car in the garage and a mechanic that you never see. The manager and the customer relations guy takes your car and makes you feel good, but the mechanic does the work.

We have such a witness, Mr. Kie Fallis. And, Kie, if you would sit at the end of the witness table, I would appreciate it. Mr. Fallis is a former Army interrogator. He is fluent in Farsi, he is an Iran specialist, he spent one year with the FBI investigating the Khobar Towers situation. He is an expert in recognizing the computer software analytical capability and workable databases. Using his background and training and ability, Mr. Fallis provided what has been labeled an Usama bin Ladin blueprint of various methods and connections. The result: the same terrorists who planned the previous attacks were also planning the next attack. He received a distinguished performance rating from the DIA in July 2000.

Mr. Fallis then tracked the al-Qa'ida for a year, linked them to Iranian intelligence and terrorist cells. In January 2000, he predicted two or three major attacks against the United States. He noted that the broadcasts by UBL are followed by attacks. He made the connection to Iran and that connection resulted in the infamous 2000 Malaysia meeting of the al-Qa'ida, some fellow by the name of Mihdhar and some fellow by the name of Hazmi, those linked to the *Cole* attack and later also the 9/11 attack. He attempted in vain to convince his superiors to issue a threat warning in August of 2000.

Mr. Fallis basically analyzed two warning streams of intelligence reporting, the al-Qa'ida and Iran, and tried to get his draft warning report approved. His warnings were considered, I think they were called anomalies, not connections. We now know different. The DIA issued the warning the day after the attack. Mr. Fallis, acting out of conscience, citing significant, very different analytical differences, then resigned the day after the *Cole* attack. Upon request, he did provide this committee and the Armed Services Committee valuable insight and suggestions at the time of the *Cole* investigation. He is now an intelligence consultant.

I would like to bring to the attention of my colleagues a book called Breakdown, by Bill Gertz, a local and respected reporter. On pages 31 to 59 you have the saga in regards to Kie Fallis and what we should have learned. Mr. Fallis has prepared testimony today citing three notable differences between various analysts in the Intelligence Community and several recommendations in behalf of all the hardworking analysts who, in his words, represent the linchpin of our Nation's ability to predict all future events and to warn the policymakers of important and very crucial developments in the world.

Mr. Fallis, please feel free to summarize your statement. I have just a couple of questions following that if we have time.

[The prepared statement of Mr. Fallis follows:]

Statement for the Record

Lessons Learned and Actions Taken in Past Events

8 October 2002

Kie C. Fallis

Introduction

Chairman Graham, Chairman Goss and Members of these Committees: Thank you for the opportunity to address the issue of lessons learned and actions taken in past events. My comments of this subject will be addressed from the perspective of a counterterrorism analyst formerly assigned to the Defense Intelligence Agency. The many dedicated analysts in the Intelligence Community are the lynchpin of our nation's ability to successfully predict future events and to warn policy makers of important developments in the world. Successful intelligence analysis by itself is not extraordinarily difficult nor does it push any intellectual boundaries. It is a learned and trained process augmented by a background in a given field, and then developed through analytical software tools, databases and collaborative human minds. To accomplish this, an analyst must read and be familiar with as much information about their target as possible and to then communicate that knowledge in an effective and timely manner to their customers. When the situation warrants it, they will contribute to a formal warning process. As a subject matter expert in a given field, the analyst is also that person primarily responsible for identifying gaps in information and properly tasking the intelligence collection systems to gather the needed data. If the analysts fail to do their job, fail to read the collected intelligence, or fail to follow up on obvious intelligence gaps, the entire intelligence cycle will grind to a halt. The chances that we will be able to predict or prevent the next major act of terrorism are reduced to little more than dumb luck. However, with the proper tools, training and mandated sharing of intelligence information with properly cleared personnel, we will do better.

Terrorism Analysis as a Unique Field

There are significant differences in methodology between an all-source analyst studying a terrorist group and other all-source analysts in the Intelligence Community. These differences can potentially complicate accurate assessments and warnings, but are frequently not recognized even inside the counterterrorism community itself. While these differences need to be taken into account when examining past successes or

failures, they do not necessarily make the terrorism analyst's job any more difficult than their counterpart's.

The first, and arguably most important, distinction is the bureaucratic level at which meaningful advisories and warnings are communicated to intelligence consumers and to policy makers. In the case of a political/military all-source analyst, the closer the collector and/or analyst is to the subject the more likely they will be able to provide tactical warning of an upcoming event. For example, forward-deployed military intelligence units currently in Afghanistan will probably develop the critical details of an upcoming conventional attack against US interests, the who, what, where and when, before CONUS based analysts. This is due to their being physically on the ground with established liaison relationships, and by being able to exploit in-theater collection assets. Although this is a generalization and there have been several exceptions, most in the Intelligence Community do not expect DC-based analysts to provide specific tactical warnings of conventional attack to deployed units or to our Embassies abroad. They instead expect, and receive, strategic level assessments of recent activity and broad predictions of future actions. In the area of terrorism analysis, this recognized hierarchy is turned upside down. As this committee has already seen, a great deal of pertinent intelligence on terrorists and terrorist groups is collected, maintained and not adequately shared by, or even among, the major intelligence agencies. The more accurate and timely information is frequently retained by these agencies and not passed down the chain. When it is passed, the information is often watered-down or generalized in an attempt to protect sources and methods, as well as the need-to-know principle. There are numerous examples of this happening in the past and I will briefly discuss a few of them in another section. Consequently, our men and women assigned abroad for the State Department and the military are usually capable only of noting the broad details of a terrorist group's activities and are therefore more likely to be able to discern only strategic indicators of an upcoming attack.

The second notable difference between terrorism analysts and their all-source counterparts concerns the type of information available for incorporation into assessments and other intelligence products. Many all-source analysts are directed at subjects such as a nation-state, or some aspect of that target's capabilities where the

existence, location, leadership, etc is not hidden or in dispute. When examining these types of subjects, the potential sources of accurate information cover a wide spectrum from academic and press reporting to highly sensitive intelligence information. This is not usually the case with terrorism analysis. Since almost all terrorist groups, and certainly their operational cells, function in a closed, clandestine manner potential sources of accurate information are almost always limited to sensitive intelligence reporting. As a result, the terrorism analyst must work harder over a longer period of time in an effort to corroborate reporting and build an accurate profile of a group.

The third difference also concerns collected information, but is focused on the method by which the two types of analysts assess its veracity. Most all-source analysts take advantage of their wider spectrum of information in order to more easily verify its truthfulness. This variety also decreases the amount of experience and area knowledge needed by the analyst to correctly weigh the reporting. As noted above, the terrorism analyst is constrained, not by the volume of reporting, but usually by the number and types of sources. This lack of variety can cause problems when trying to verify current reporting in a timely manner and has a potentially negative impact on the warning process.

Terrorism Analytical Issues Complicating Improved Future Performance

The single most important issue that will affect future performance is the experience level of the analyst. While this certainly applies to all intelligence analysts regardless of subject area it is even more critical for those trying to prevent the next terrorist attack. In the case of an analyst responsible for tracking a Middle Eastern terrorist group, this person will need to have an expertise, or at least a good working knowledge, of terrorism itself and the group, regional and country issues present in the group's operating area and Islamic history, culture and sects. As of October 2000, the Middle Eastern terrorism analyst who could claim that level of knowledge was by far the exception. For example, most new civilian hires and assigned military officers to DIA's Office for Counterterrorism Analysis lacked expertise in even one of these fields, much less all three. This was certainly not the fault of the DIA which was actually ahead of the

Community in attempting to hire additional analysts. The required levels of experience are almost never found in the civilian/academic world and are instead developed over time by training programs and in-house mentors.

Lack of experience has another impact on the terrorism analysis effort; namely the inability to consider current intelligence reporting in its proper historic perspective. In the period leading up to both the 1998 East Africa Embassy Bombings and the 2000 attack against the USS Cole in Yemen, terrorism analysts incorrectly assessed that a group would not conduct an attack in an area where it was able to operate with relative ease. Additionally, there appears to be a continued reluctance to correctly assess and evaluate the nature of cooperation between many Sunni and Shi'a Islamic extremist groups. Both of these examples, and there are certainly others, occurred despite over a decade of credible reporting to the contrary.

As the amount of information collected against al Qaeda and other terrorist groups continues to increase, each and every terrorism analyst must be given the tools to properly database that information. These tools do not necessarily need to be uniform, and the way an individual analyst uses the tools to improve his or her results will probably also vary by agency and mission. However, they must be used. The fragmentary and periodic nature of intelligence reporting on terrorism targets spans several years and cannot simply reside in an analyst's short-term memory. The frequent use of ever-changing actors, aliases and codewords is another unique challenge and significantly increases the chance of confusion and incorrect assessments. Only by carefully evaluating the veracity of collected information, properly noting its historic context (recent or otherwise) and then cataloguing it in a database tool will a terrorism analyst have any chance of connecting all the dots. Databases that also have the means to graphically represent their data will simplify and improve collaborative efforts with other intelligence analysts.

The other significant issue complicating future analytical performance against terrorists is the tendency of the FBI to compartment all pre- and post-attack investigative information. I realize this committee has spent a great deal of its time looking at the many legal and other aspects of this problem and I am not qualified to comment on those findings. However, as a former terrorism analyst and liaison officer to the FBI I can tell

you that having this information is critically important to being able to predict a future event. If the Community's analysts are left in the dark about how a group puts an attack together, and each group tends to do things a little differently, how will those analysts be able to pick up on future indicators? The investigative results of the 1996 Khobar Towers bombing were not disseminated until almost two years after the event and then only to a few select analysts and agencies. As a result, many analysts have incorrectly assessed al Qaeda as being culpable in this attack. These incorrect assessments in turn influence other products. Furthermore, since some of the individuals connected to this attack remain active in terrorism reporting, if an analyst is unaware of that person's role in a previous attack he or she will probably fail to attach the proper level of importance to that person's current activities. In another unfortunate example, US agencies conducted a vigorous investigation, to include a physical search, of the al Qaeda cell leader in Nairobi nearly a year prior to the 1998 Embassy bombings. Almost all of the results of this effort were never shared with the terrorism analytical community due to concerns about the criminal case. Most of the information was never properly exploited. In fact, a great deal of it was only translated after the bombings themselves. After the Embassy bombings, the post attack investigative results were again not shared. By failing to share this information, Bin Laden analysts were unable to build a correct modus operandi for al Qaeda attacks, and like the Khobar Towers example, they were unable to attach the proper level of importance to those culpable individuals still at large. This directly contributed to most analysts having only a moderate level of interest in the January 2000 Malaysia meeting of al Qaeda operatives, when in fact the same node that had organized a great deal of the East Africa Bombings was again active in organizing the Malaysia meeting.

Terrorism Warning Issues Complicating Improved Future Performance

The US has a well-developed and carefully thought out interagency terrorism advisory and warning system available to intelligence consumers and policy makers. The membership of various agencies, as well as the policy and procedures for issuing reports are carefully laid out and easily understood. In DOD's case, this interagency system is

augmented by its own which it can use separately or in conjunction with the other. Of note, DOD units at every level retain the authority to issue warnings if necessary. The ability of the US counterterrorism community to accurately predict and/or prevent the next terrorist attack against US interests should be priority number one and should be reflected in the quality of the warning products it issues. Unfortunately, inconsistent and vague advisories/warnings appear to have slowly diluted the system's effectiveness. Frequently, advisories have been issued not based upon the development of credible threat information, but rather upon the size or importance of an upcoming meeting, such as a gathering of major world leaders or a large sporting event. There are also inconsistent thresholds for issuing warning products among the major agencies. Some organizations appear willing to postpone an advisory until more complete information is received, while others will issue a warning based upon a single poorly-sourced intelligence report. These inconsistent thresholds are also usually apparent to the intelligence customer. In addition, there has been an inexplicable tendency on the part of some intelligence agencies to issue warning reports and raise the terrorism threat level after an attack.

As I noted earlier, most intelligence relating to terrorist groups is vague and fragmentary with the complete picture of a potential attack only developing after a period of several months, or even years. The fact that this information is vague should not deter warning officers, because when examined together the totality of the reporting usually results in a more complete and corroborated threat scenario. This is precisely what happened in the months leading up to the USS Cole attack. Almost all of the information required to predict or prevent this attack existed in intelligence databases, but since that puzzle had been in the process of being put together for almost a year, warning officers failed to appreciate the gravity of the last few reports on this subject since those reports did not appear to be out of the ordinary. This step-by-step approach to threat warning is the only realistic method available to us. The chance that our intelligence collectors, as good as they are, will stumble upon the who, what, where, when and how of a terrorist attack and then publish it in one or two messages is highly unlikely. Waiting for such a message is foolhardy.

Conclusion

The collection of additional information, further reorganizations and the hiring of additional analysts is unlikely to significantly affect any of these issues. The central hub in our nation's past, present and future failures or successes in the counterterrorism arena will rest squarely on the shoulders of the working-level analysts in both the law enforcement and intelligence communities. These men and women are the hard-working patriots who will have to try and find that single piece of hay in a stack of needles, and then try to tie it to another disparate piece of information in a timely manner. This will never be an easy job for them to accomplish, but the leadership of America's intelligence and law enforcement communities must provide them with the training, tools and information to accomplish the mission. The information they need to successfully predict and prevent the next terror attack is probably already contained in one or more community databases. The only question is whether experienced, working-level analysts will be given access to that information and will properly integrate that material into an accurate advisory or warning.

TESTIMONY OF KIE FALLIS, INTELLIGENCE CONSULTANT, FORMER TERRORISM ANALYST, DEFENSE INTELLIGENCE AGENCY

Mr. FALLIS. Thank you, Senator Roberts.

Mr. Chairman, members of these committees, I would like to tell you that it is a great honor for me to come before you today to have a discussion about the subject at hand. I would also like to say it is a great honor for me to be a part of this group of distinguished Americans at the table here as well. That said, my comments today will be strictly from the perspective of a former terrorism analyst employed at the Defense Intelligence Agency. What I would like to do is just to briefly summarize my written statement, and I want to move sort of immediately to this part on Terrorism Analytical Issues Complicating Improved Future Performance.

The single most important issue that will affect future performance is the experience level of the analyst. While this certainly applies to all intelligence analysts regardless of subject area, it is even more critical for those trying to prevent the next terrorist attack. In the case of an analyst responsible for tracking a Middle Eastern terrorist group, this person will need to have an expertise or at least a good working knowledge of terrorism itself, the group that they have for an account, regional and country issues present in the group's operating area, which can be quite extensive, and Islamic history, culture and the sects thereof. This sort of required level of expertise is rarely going to be found outside the Intelligence Community and is instead going to be recruited from academia and then developed in-house through training programs and mentors.

Coupled with this issue of experience comes the ability to place current intelligence reporting in the context of historical perspectives. In the period leading up to the 1998 East Africa bombings and the 2000 attack against the USS *Cole* in Yemen, terrorism analysts nearly across the board incorrectly assessed that a group would not conduct an attack in an area where it was able to operate with relative ease. Additionally, there appears to be a continued reluctance to correctly assess and evaluate the nature of cooperation between many Sunni and Shi'a Islamic extremist groups. Both of these examples, and there are certainly others, occurred despite over a decade of credible reporting to the contrary.

The other significant issue complicating future analytical performance against terrorists is the tendency of the FBI to compartment all pre- and post-attack investigative information. I realize this committee has spent a great deal of its time looking at the many legal and other aspects of this problem, and I am not qualified to comment on those findings. However, as a former terrorism analyst and liaison officer to the FBI, I can tell you that having this information is critically important to being able to predict a future event.

If the Community's analysts are left in the dark about how a group puts an attack together, and each group does tend to do things a little differently, how will those analysts be able to pick up on future indicators of a future attack? Quite frankly, it is nearly impossible. As an example, the investigative results of the 1996 Khobar Towers bombing were not disseminated until almost two

years after the event and then only to a few select analysts and agencies.

Another issue would have occurred right prior to the 1998 East Africa bombings, in that U.S. agencies had conducted a vigorous investigation to include a physical search of the al-Qa'ida cell leader in Nairobi almost a year prior to this bombing. Almost all the results of this effort weren't shared with the terrorism analytical community due to concerns, legitimate concerns, about the criminal case. Most of the information was never properly exploited. And after the embassy bombings, the post-attack investigative results were not shared. As a result, by failing to share the information, bin Ladin analysts were unable to build a correct modus operandi for al-Qa'ida attacks and, like the Khobar Towers example, they were unable to attach the proper level of importance to those culpable individuals still at large.

This directly contributed to most analysts having only a moderate level of interest in the January 2000 Malaysia meeting of al-Qa'ida operatives when in fact the same node that had organized the meeting in Malaysia was in fact responsible for a great deal of the planning for the East Africa bombings.

Moving on to my conclusions, the collection of additional information, further reorganizations and the hiring of additional analysts is unlikely to significantly affect any of these issues. The central hub in our Nation's past, present and future failures or successes in the counterterrorism arena will rest squarely on the shoulders of the working-level all-source analysts in both the law enforcement and intelligence communities. These men and women are the hard-working patriots who will have to try and find that single piece of hay in a stack of needles and then try to tie it to another disparate piece of information in a timely manner. This will never be an easy job for them to accomplish, but the leadership of America's intelligence and law enforcement communities must provide them with the training, tools and information to accomplish their mission.

The information they need to successfully predict and prevent the next terror attack is probably already contained in one or more databases inside the U.S. intelligence and law enforcement communities. The only question is whether experienced, working-level analysts will be given access to that information and will properly integrate that material into an accurate advisory or warning.

Thank you. That would conclude my remarks.

Senator ROBERTS. Let me just follow up with a question, if I might. How did the use of the analytical software tools and the databases that you put together give you insight in regards to the draft that you tried to prepare improve your ability to produce the intelligence assessments on various intelligence groups, and how do we get that information to the analysts as you have just described?

Mr. FALLIS. In my case, Senator, what I did is I began to notice that there was a voluminous amount of information, as others have testified to, regarding al-Qa'ida. Most of it appeared to be unrelated to other pieces of information. It appeared to be almost chaff. By using a piece of software that I was able to have put these small snippets of information into and graphically represent them as well, I was able to over a course of many months determine certain linkages between these, these items, linkages that would never be

apparent without the use of this tool. It would simply be lost in the weeds and there were a lot of weeds to look through. The reason it makes it easier by using this and then it makes it much easier to collaborate with other analysts in the Intelligence Community, in the FBI, CIA and others, to bring your findings, share their findings and then work together towards a common goal of preventing the next attack.

Senator ROBERTS. We have heard from Ms. Hill and at other hearings that we often do not anticipate these attacks. How can we do better?

Mr. FALLIS. By making better use of the information that we've already collected, quite frankly. We have literally a treasure trove of intelligence information spanning back decades. The proper examination of that information, the proper databasing and building of relationships among—with that information I think will give us the results, not all the way to the extent that we might want them, but it will take us a lot further than we are now.

Senator ROBERTS. We have heard that in order to get the warnings out to the right people that it would represent a flood to the policymakers and others with what we call constant vague warnings or warning fatigue. How can we ensure that that doesn't happen?

Mr. FALLIS. That is a very difficult thing to accomplish, because too few warnings and the information is not going to get across, too many and you induce warning fatigue. I think the answer lies in the analytical effort against terrorist groups to be conducted more efficiently and effectively, to gather the details mined from the data that are there, put them together into a collaborative assessment and then produce better and more correct and more thorough warning products, perhaps fewer but more pressing and more accurate.

Senator ROBERTS. Senator Rudman called for bringing in outside experts on a more regular and systematic basis and our inquiries heard from others that some in the Intelligence Community at times lacked the expertise. Can these experts be found and can they be brought in to improve analysis?

Mr. FALLIS. Absolutely. That was done routinely and frequently individuals in the Counterterrorism Center, the leadership there, would attempt to bring in academic experts and others, and I would say that they contributed a lot to the effort of the Community's analysts.

Senator ROBERTS. I want to ask you a question that appears to be perhaps too basic, but how do you do your job? It is a lot like when my daughter asked me when she knew I was a Senator and she said, well, daddy, what do you really do when you go to work? I want to know how you do your job. Can you describe the type of information you use and how you put it together and what happens to it then? Just give us an idea from a typical analyst, although you are an atypical analyst from your background and your work. I thought it was prescient but I understand now that it is prescient but at any rate to that ability that you have, what do you do when you get up in the morning and you go in and you're an analyst?

Mr. FALLIS. The first thing I would generally do, Senator, would be to look through all of the national products that would be avail-

able to me in my message queue, in a computer terminal that would be sitting on my desk to sort of set the ground for what had been happening in the previous 24 hours.

From that point I would move to a message traffic handling system where I had built a profile of certain key words that would hit on certain messages being brought in. You then sometimes have up to 200 messages a day to read through. From those, I would try to pick out the most compelling information, the most accurate, the best sourced to begin populating my database with. Then throughout the day you would be talking to your counterparts at the CTC and/or the FBI and putting together assessments or other products as directed. It could be exciting and at times it could be mind numbing.

Senator ROBERTS. Is this what we call rocket science? Is this really hard work? We hear about the analyst who has to have all this expertise and background, et cetera, et cetera. You have that. You are fluent in Farsi, you are a student of that part of the world. In terms of recruiting and training, how tough is this?

Mr. FALLIS. The act of producing, of doing the analysis and producing assessments is not—it is certainly not rocket science and it certainly isn't pushing any intellectual boundaries. It does require time to build the experience to become what you would call a working-level or a journeyman-level analyst. There is nothing special about it. As I related to both committees, I certainly did nothing special in the period leading up to the attack on the USS *Cole.* I think all I did was consistently read all of the traffic I could and then instead of just moving on to something else, taking the traffic and trying to exploit every piece of information in it to see where that would take me.

Senator ROBERTS. Bottom line, do you have a recommendation in behalf of all your analyst colleagues out there who are doing the hard working work as opposed to all of the very important and necessary officials that we normally have here who testify?

Mr. FALLIS. I would say that we need two things increased, two areas of concern that are going to have to be addressed, and that is the ability of analysts across the Community to collaborate on their efforts and, in doing this collaboration, to have the most possible information available to them. Obviously we have to be concerned about whether people are properly cleared. They have to be, in order to receive certain information, read into certain programs, but by reaching that sort of apex, of good, experienced, hard-working analysts with the tools they need to do the job, I think that we will have a lot of the information to predict the next act of terrorism.

And more importantly, even now looking back at the information that we had, many people will say, well, that was too vague, that wasn't quite enough, that didn't point to this. That is absolutely true. But if it had been put together and if the gaps had been properly tasked out to collectors to follow up on and to exploit, there is no telling where that could have led to.

Senator ROBERTS. I appreciate it. Thank you, Mr. Chairman.

Chairman GOSS. Thank you, Senator. That brings an interesting dimension to the presentations today.

Ms. Pelosi.

Ms. PELOSI. Thank you very much, Mr. Chairman. Once again I want to welcome our very distinguished witnesses. Thank you for your testimony and, more importantly, thank you for your service to our country.

My questions center around the idea that immediately following September 11 it appeared that the hijackers had come into our country, they were sort of like automatons, they went to their station, they waited for their signal and they acted when they received it. From your experience, Judge White and Judge Freeh, knowing what you know about the World Trade Center bombing initially in 1993, the East Africa bombings, and the *Cole*—I am separating those from Khobar for the moment—knowing of those three which we have identified as al-Qa'ida, do you think that there was more aid and comfort in the United States in the network that they hooked up with when they got to the United States?

I'm trying to evaluate what the threat is for the future as well as find out how this happened. We owe the families some answers, some comfort, and we want to reduce risk to the American people. We are trying to evaluate what is out there.

Judge FREEH. I'll try to answer the question. Of course I'm not privy to most of the non-public, in fact any of the non-public facts relating to September 11. In fact, that is why I quoted from Director Mueller's statement because those are the facts as I understand them.

Ms. PELOSI. I just meant based on what you knew about East Africa and *Cole.*

Judge FREEH. Let me give you a couple of examples. In the East Africa embassy attacks, two principles which I think are very important and relevant to September 11, one, the people who were selected for those missions were for the most part innocuous players—they were fishermen and store clerks who lived in communities, who had roots in many cases, and were ordinary and non-obvious people even in the societies where they had operated and lived for many, many years.

What they had in common was the al-Qa'ida connection and the ability to become operational. Going back to the World Trade Tower, which Ms. White discussed in detail, they lived in the community. The Blind Shaykh preached in mosques in Jersey City and in Brooklyn, New York. These were not extraordinary lives in terms of proved up or even known connections to international terrorist groups. There was some training involved, obviously, and much of it learned after the fact with respect to Yousef- and al-Qa'ida-sponsored training operations, but for the most part they were never linked per se to an international terrorist organization.

I think the dynamic there is the selection and the preparation. Also in East Africa, one theme which was repeated in the *Cole* attack is these are people who planned for years, who painstakingly did surveillances, who quietly did many, many things in preparation. As you know, in the *Cole* attack the target originally was another ship, the USS *The Sullivans,* an attack which was going to coincide with Ressam's activity on the West Coast and the al-Qa'ida cell attacking Americans and Israelis in Jordan. So very painstakingly planned by ordinary people with very patient and time consuming operations.

Ms. PELOSI. Thank you, Judge Freeh. Judge.

Ms. WHITE. I agree with what Director Freeh said. One of the remarkable things about 9/11 I think is how much of the planning occurred abroad, which obviously points out how critical holding onto that world coalition of partners is in the fight against terrorism, and what was done within the country were just routine living acts. So I certainly don't see from what I know a suggestion of aid and comfort within the United States.

I will say, and I don't know how these facts will pan out, but two of the recent series of arrests in Buffalo and I guess Detroit, I think, that actually troubles me the most since I have left office in terms of what that can mean. In other words, if you have got cells within the country, second generation Americans, assuming that is so and obviously it remains to be seen who are—really are sleeper cells from within the country. That I think poses quite a danger if the facts turn out to be that.

Ms. PELOSI. My time is expiring. I just want to say, Mr. Director, Judge Freeh, that I was pleased that you mentioned John O'Neill in your opening comments. I visited with him the day in June of 2001 that he had just come from the airport, at 2:00 a.m.; I met him about 9:00. He was debriefing some of the agents who had come back from Yemen that day. Of course he was full of that story and also full of knowledge of Usama bin Ladin and his designs on the U.S. I can't help but think how things might have been different after September 11 if we had some of the benefit of his thinking to unravel some of this, to understand the threat that still remains in the U.S.

Judge FREEH. I agree. It was so tragic and ironic—probably one of the individuals in the world most knowledgeable about this organization and its operations, killed as he is trying to save people that day along with many other heroes. Very, very tragic.

Ms. PELOSI. I wondered if he had known about the Moussaoui tape and the Phoenix memo and the rest of that. I don't know if he knew about it or if he left the agency before that information came to the fore, because he seemed to be a person who had judgment about those issues.

Judge FREEH. He was an excellent agent and investigator. I don't know the answer to your question, though.

Ms. PELOSI. Thank you again for your testimony and for your service. Thank you, Mr. Chairman.

Chairman GOSS. Senator Shelby.

Vice Chairman SHELBY. Thank you, Mr. Chairman.

Judge Freeh, I have a lot of respect for you and have worked with you when I was chairman of the committee for a number of years, closely with Senator Kerrey and Senator Bryan and others, but the picture you have painted here today, not all of it but some of it, regarding the FBI is not the same picture that our investigative staff has found, discovered or what we have been hearing, not in all respects. In some, yes. Because we do know that the FBI under your tenure did a lot of good things. But that is not our job to just ignore the others. The Wall Street Journal article today, which took an extract from your statement, says the FBI did its best. I don't doubt that. But that is not good enough. We are going

to have to do better. That is what we're talking about. And we want to do better.

You also mentioned, and correct me if I am wrong on this, my perception of what you said, that the FBI and the CIA, they were speaking to each other, that they, yes, more and more. And we know there has been cooperation, some cooperation. Historically not, but in recent years, in the eight years that I have been on this committee, I have seen a lot. But I have seen a lot of problems.

Let me just point out some situations, just go over them again just for the record—the lack of sharing of information, the Phoenix memo, the Phoenix memo we keep talking about. A lot of us believe that is a very important piece of information. It was never seen by the FBI headquarters, in other words, the higher-ups. I don't know if you had left by July 10. Had you left by July 10?

Judge FREEH. Yes, sir.

Vice Chairman SHELBY. It was never disseminated to the CIA. The Transportation Security Administration said they never saw it. On a local level, the information you were asked earlier about by Congressman LaHood, Commissioner Norris, who is the Police Chief at Baltimore, testified here under oath that the FBI never shared information on terrorist investigations that were ongoing locally in Baltimore. The Transportation Security Administration testified here under oath that they never got background on terrorist activities or scope from the FBI. Governor Gilmore, the former Governor of Virginia that you know well, testified about the lack of sharing from the Intelligence Community, not the Bureau, to State and local officials, testified that as Governor he never got briefings on terrorist intelligence from the Intelligence Community. He did not mention the Bureau.

I do believe, Mr. Freeh, that the FBI and the CIA still have information-sharing problems as we speak, right this minute. There is no central place where there is a fusion of terrorist information, all information going into one center, about anything. That is a real problem.

The CIA, you are talking about sharing, it goes both ways. The CIA has some of those problems, too. The CIA did not give the FBI visa information on al-Mihdhar and al-Hazmi and the fact that they were traveling to the U.S.—very, very important information. The CIA missed several opportunities to do so—in January of 2000, March of 2000, June of 2001. At the June 2000 meeting between New York FBI agents on the *Cole* investigation that Senator Roberts has focused on and the CIA, the FBI agent testified here behind the screen that CIA showed them photographs of Mihdhar and others but refused the FBI request, and this was a Bureau request, for copies of the photographs, more information on why the people in the photographs were being followed and so forth. At the meetings, the CIA did not tell the FBI about the fact that Hazmi had traveled to the U.S. and al-Mihdhar had a U.S. visa.

This is a serious lack of sharing of information. They have shared, I am sure, but these are the troubling things. I know my time is up.

The other thing that is troubling to me, and maybe you can talk about it and I will stay around for another round, you mentioned in your remarks Saudi cooperation, the government. I recall, and

the record will reflect that in the committee, that you told us in the committee on several occasions dealing with Khobar Towers that the problem, the impediment early on, maybe it improved, in the investigation of Khobar Towers, one of the problems was the lack of cooperation by the Saudi government.

Judge FREEH. Yes, sir.

Vice Chairman SHELBY. Is that correct?

Judge FREEH. Yes. Let me answer both of your questions. Yes, at an early point there is no question—and I reflect that in my statement—there were a lot of obstacles, some that were legal, some that were cultural, some were due to the fact that we were trying to make that liaison work from Rome for many years, which is completely impractical. What I also briefed you on during the course of that case, which was several years, is that slowly but in a very, very positive fashion and ultimately resulting in the type of access that I testified to this morning, they did exactly what we asked and they did it at the expense of their own interests. That is my opinion.

Vice Chairman SHELBY. But it took a while to do that, didn't it?

Judge FREEH. It surely did, which is why those liaisons are so important. If I had had an FBI agent in Riyadh on June 25, 1996, when that tragedy occurred, who had the trust and a relationship that the Legat had three years later when he set up the office, I would have done much better.

With respect to your other question, there is no doubt that all those points that you raise are troubling points. As I mentioned this morning, the committee has done an absolutely fair and excellent job in going back, as it should, and finding and highlighting those points. My caveat, however, and my strong suggestion to this committee is that you cannot highlight and isolate those specific lapses and exclude and ignore the excellent relationship that exists between the FBI and the CIA. I think to do that is a disservice to the relationship, and it is not accurate. It is not my experience, it is not this committee's experience.

As I have said before, I heard nothing in the eight years from any member of either committee that did not confirm my own experience that this was a very productive, efficient and transparent relationship, not to say that there were points and gaps. We ought to identify them. You have identified them. We should fix them. But to highlight those to the exclusion of everything else I believe, my opinion, is not accurate and not the picture that is relevant to my experience.

Vice Chairman SHELBY. But the facts are the facts?

Judge FREEH. The facts are the facts. But there are the facts which are points among thousands and thousands and thousands of other points relevant at that time. I think we need to fix them and correct them and highlight them, but if you just connect those ex post facto, that is not the experience or the reality that I remember.

Vice Chairman SHELBY. Thank you, Mr. Chairman.

Chairman GOSS. Governor Castle.

Mr. CASTLE. Thank you, Mr. Chairman.

Let me address this question, I guess, to Mr. Freeh. It is a very broad question but it is something I am interested in, but the oth-

ers may chime in if you have good answers. This is my concern. Setting aside any questions about what the FBI did or did not do before September 11, and looking at the history of the FBI all the way back to Hoover and its pursuit particularly of criminals in America, et cetera, it just seems to me that there is—I am not being critical when I say this at all of anything that has happened of the FBI or anybody else—it just seems to me that there is a little bit of a disconnect between what the FBI does and the CIA does and just because we say when they cross our borders and therefore the FBI is going to be involved and not the CIA is necessarily the right answer as far as I can see.

When I look at the CIA, I did realize their ability. I wish they had more in languages and culture and knowledge of political situations or whatever, and these are things that in my judgment the average, heretofore, the regular FBI agent being trained really did not necessarily have. Without retroactively being critical of what has happened, do you have any thoughts or suggestions about the total structure?

One of the things we need to do is determine how do we go forward in the future. What is in the best interests of America? I am not totally sure that the system did work that well because it has structural problems, not because of any failings of individuals or lack of communication or whatever it may be, but there just might be structural problems in terms of what the responsibilities are. To some degree I think, of all the ones that are a little more a fish out of water, it might be the FBI in that circumstance. Again, that isn't criticism. But do you get the drift of my question?

Judge FREEH. I think I do. Let me see if I can answer it this way. We're not immune to criticism and we should be criticized for some of the lapses and gaps.

Mr. CASTLE. I'm not worried about all that.

Judge FREEH. Let's talk about your question then if I can. I think the way to characterize it, the Counterterrorism Program is a unique program in this respect. At least when we're talking about international terrorism, we're talking about intelligence collection, primarily overseas but also in the United States, and we're talking about law enforcement.

There is a disconnect between the FBI and the CIA. It is called the National Security Act of 1946, a decision to prevent the CIA from becoming a domestic intelligence agency operating in the United States. Congress made that decision. I think it was a great decision then. I think it is a relevant decision now. The counterterrorism program, unlike the organized crime program, unlike the counterintelligence program, is a fairly new program. This was a program that started around 1990, 1991, 1993. Just look at our history of appropriations. We haven't been doing this a long time. We have been doing organized crime for several decades, counterintelligence for more than that, and bank robberies and investigations for 90-plus years.

So there are some structural issues with respect to the administration of the program and the efficient coupling of our collection abilities overseas which are primarily the Agency's, not the FBI, and melding that together into a prevention program, which it should be primarily, but also an enforcement program.

I don't think frustration that this has not worked as well as some other historical programs should result in the conclusion that, well, we have to do something radical, like set up a domestic intelligence agency which, and I agree with Senator Rudman, would be a huge mistake in my opinion. I think what we have to do is resource it, integrate it; going back to Senator Shelby's questions, make sure we have a point where all the information flows and is retrievable and is mined and is utilized.

But this is very, very hard. And I think the last point I make in response, this is very, very hard. It is not, as I was speaking to the Chairman before the hearing, it is not like you go into a room and there is a machine and you press a button and you get all the data possibly available in one place analyzed with some suggested leads. We may get to that point and there may be some technology or software that gives us that ability, but there is no such thing.

So there is always going to be gaps. There are always going to be points of light. There are always going to be intersections where something falls off the track. The comeback to that is redoubling our efforts, resources, training, technology, integration, changing the structures around. I don't think we have to reinvent the wheel.

Mr. CASTLE. Let me ask a quick question so I don't run out of time. I don't disagree with what you're saying, but sometimes I wonder. Counterterrorism is fine and that kind of thing, but even if we don't separate it from the FBI, should the FBI be divided more so that there are people who focus just on this and there are people who focus just on, say, crime in the United States? I'm a little worried about the other aspects of the FBI being harmed by all this, too, that all of a sudden the scales have gone so drastically the other way that we are forgetting the other functions of the FBI, too.

Judge FREEH. The answer is we have a division, we have a Counterterrorism Division.

Mr. CASTLE. Is it really divided sufficiently you think at this point?

Judge FREEH. We can do better. It's a new creature within the structure. We have a Counterintelligence/National Security Division. We have a Criminal Division. We have all these things. I think the organization is there and, as Senator Rudman said, the expertise in terms of the collection and the protocols necessary for enforcement and prevention are there. We have just got to resource them and integrate them in a better way.

Mr. CASTLE. Thank you, Mr. Freeh. I yield back, Mr. Chairman.

Chairman GOSS. I have a couple of questions which have been stimulated by the conversations today which have been very helpful to me. The first one basically goes to Judge Freeh, your remarks that we are a Nation that is a rule of law Nation and we are very proud of that. We are a free, democratic and open society.

And I would be interested to know what you and Ms. White and Dr. Pillar would say to the question that we play by the Marquis of Queensberry rules and the other guys don't. Is there a simple way that we could deal with that?

Dr. PILLAR. Not a simple way, Mr. Chairman.

Chairman GOSS. How far can we go, understanding that we're getting hit below the belt, but we will not hit below the belt?

Ms. WHITE. The rules are different, depending on what system we're using, to some extent. If you're talking about the criminal justice system, I would be the last person to advocate treating a terrorist defendant any differently than any other kind of defendant, despite the seriousness in the crimes and the difficulties in doing that, or we dilute our own system.

Chairman GOSS. Well, I would put it a little differently.

Let's suppose somebody comes into this country with malice aforethought and they are going to do a dastardly deed such as the World Trade Towers, but they don't break any laws and they don't have any fear of the death penalty because that's their reward.

How do we make our law enforcement and our intelligence defensive capabilities work to figure out how we can stop something before it happens in a case like that? What authority do we have and what capability do we have here in a free, democratic, open society to say, "Gee, we're the Thought Police; we think you're thinking of doing something bad. You're treated as an American person here, and we're a little concerned about that?"

Ms. WHITE. Well——

Judge FREEH. Well, I would agree with Mary Jo White that we've got to talk about what plane we're operating on. If it's an immigration issue and a border issue, you know the person doesn't have the same rights, obviously, and the same ability to even the remain in the United States that a U.S. person would have.

Should we use a law enforcement agency to operate, to use your phrase, as the Thought Police or a preventive police? You know my view is no.

If we have a suspected terrorist who has in his mind plans to commit an attack, should we allow the FBI to use whatever measures possible or available to get that person to disclose that information? Many countries, as you know, do that. Do you want your FBI agents doing that? And then who chooses the cases where that technique is used and not used? These are huge and difficult issues.

I think I come back to the FBI, at least, being part of the Department of Justice and being an agency that adheres to the rule of law.

Now, the Congress, the courts, the Attorney General and the President can change those rules from time to time. I'm looking here at the draft of the new Attorney General guidelines on general crimes and domestic terrorism enterprise investigations, a completely different document than we operated under for eight years. That's fine as long as those rules are changed, of course, with the rule of law and they're clarified; and then you and others scrutinize how they're operating.

Chairman GOSS. Well, the reason I was asking is because that's exactly the process we're in, is scrutinizing those kinds of questions now. I mean, we're hung up on the question of how do you deal with these people once you catch them and even do the document exploitation? Are they detainees, war criminals, depending, et cetera—all of the combination of citizenship that could be involved in all of that? How far can you go asking questions and does it depend on an urgency that something horrible is going to happen if you don't get the right question asked soon of the person who has

that answer and doesn't want to give it to you? Those are very difficult questions.

Judge FREEH. They're extremely difficult.

Chairman GOSS. We're looking for ways to legislate a solution or point to the executive branch to say, do something; you've the people that have had that experience.

Dr. Pillar did have you any point on that?

Dr. PILLAR. Just if we can catch the person overseas first, there are things that we would do there or have our foreign partners do, still short of committing anything that would be a human rights abuse or that would offend our values, in those respects, but would still not be the sort of thing that the FBI or U.S. attorney would do here—things that would fit under the category of, shall we say, "harassment" or even just a knock on the door by the local police or security service is enough—and we have seen it happen in the past—to break up an incipient terrorist operation.

Terrorists don't like to be found out. They don't like to be suspected. So there are a lot of things that we can encourage our foreign partners to do just under the mere suspicion that perhaps the FBI could not do here in the United States.

Chairman GOSS. I would just simply say, is it right for to us do get a third party to do what we ourselves would not do?

Dr. PILLAR. Again, I would emphasize I am talking about things that would fall short of anything that would be a human rights abuse or things contrary to our values, but they would still fall into the harassment category.

Chairman GOSS. Not to be contentious, but just suppose we talked about, we know where your family is.

Dr. PILLAR. That's a possibility——

Chairman GOSS. That's a possibility?

Dr. PILLAR [continuing]. As a mind game.

Chairman GOSS. Well, it's exactly the kind of question. I mean, defining terror, defining all of these words that we are going into a new global time.

We know who we are, we think. How do we act in the world to best represent who we really are? That's sort of the question we're wrestling with.

Dr. PILLAR. There are a lot of things we can do that I would categorize as mind games—no use of force, no use of violence, certainly no abuse of human rights—that can be, and have been, effective as a disruptive tool with terrorist infrastructures overseas.

Judge FREEH. Mr. Chairman, again I think it goes to the earlier discussion and point that was made here by, I think, every witness today. You know, what world are we in? If we are fighting a war, you know, we're using different rules and different remedies. If we're conducting a criminal investigation, we're doing something else. But, you know, the tip of the spear of the country's counterterrorism policy is not found in an arrest warrant from a grand jury in New York. It's going to be found at the tip of a TLAM missile in that category of threat. So we have to know what world we're in and follow those rules.

Chairman GOSS. Well, again, my time has expired, and I agree that we do have to know that. That process itself is difficult. We

had war declared in 1998 against us and by us and nobody came, which we'll get to in my second question in the next round.

I think we are going now to Mr. LaHood.

Mr. LAHOOD. I just have one question. You've been very patient with all of us. I appreciate that and I know all the Members do.

I asked Director Tenet this question, and I ask it of you because of your long and many years' experience in dealing with issues of terrorism:

What was your reaction—not your emotional reaction, because I know, Judge Freeh, you mentioned the victims right in the beginning of your testimony, so I'm sure we know what your emotional reaction was. But on September 11, what was your reaction when you discovered that four planes had been commandeered and 3,000 Americans had been killed, four planes simultaneously?

And I'm asking that in the sense of were you surprised or—and I don't want you to—I'm trying to determine if you know this idea, that this could happen, was a surprise to you like it was to every Member of Congress and every American. Or was this idea—I mean, you've talked about the fact that you knew America was going to be attacked again, and we know it's going to be attacked again. But I'm wondering what your reaction was when you saw the pictures on the television screen and thought about what happened.

Ms. WHITE. I was actually there so I actually saw more than on the television screen.

My reaction was like all of America's, horror in the manner in which the attack occurred, and the massiveness of it came as a surprise to me too—not that there was an attack, not that there was a massive attack, but as massive as it was and in the way that it was.

What's the phrase everyone uses now, which I think is apt for my reaction? Is it "a failure of imagination"? Maybe it is, but I was surprised at the attack, the type of attack.

Judge FREEH. I would say the same thing. The scope of the attack, but not the fact of the attack, you know, was shocking.

We were all, I think—towards the end of 1999, literally the last days and minutes, we were all in our respective command posts around the country. You probably remember this was the Millennium where we weren't only worried about the computers turning over, but we were worried about a major attack by either an al-Qa'ida-type group or some other organization either in the United States or somewhere around the world.

An attack that would have happened at that time would have not surprised anybody. There wouldn't have been any shock with respect to the fact that we were attacked. And again, this is coming down the road from the World Trade Tower, from Khobar, from the East African embassy bombings.

So, in answer to the question, the scope of it and the success of it, I mean the horrific success of it, but not the attack itself, was a shock.

Dr. PILLAR. With regard to any particular technique, by definition, it's a surprise, because if it could have been foreseen tactically, it would have been headed off.

But as to an attack aimed against the U.S. homeland to cause mass casualties, truly mass casualties, and by this particular group, or people of their ilk, in that sense it's not a surprise.

Mr. LAHOOD. So should we worry that it will happen again?

Dr. PILLAR. Yes, sir.

Mr. LAHOOD. Judge Freeh?

Judge FREEH. Absolutely.

Mr. LAHOOD. Ms. White.

Ms. WHITE. Yes, we should worry about it.

Mr. LAHOOD. Thank you, Mr. Chairman.

Chairman GOSS. Mr. Roemer.

Mr. ROEMER. We talked a little bit about how we try to anticipate what happens next. Following up on Mr. LaHood's question, how do we try to prepare our country and our intelligence services and our law enforcement and our local responders for what might happen next in the country?

I guess, in reading a book that was written about Pearl Harbor by Roberta Wohlstetter, she has a preface in it written by Thomas Schelling, and he says—in his preface to Pearl Harbor, he says this was a national failure to anticipate the enemy's next move.

Many people in the press have speculated that there are smoking guns or, you know, old adages that we apply. How would you respond to that, Judge Freeh, that this was a national failure to anticipate the enemy's next move when we were at war?

Judge FREEH. Well, I think you know this committee's work and any commission to follow is going to have to give us a lot more facts and perspective to make that kind of a conclusion.

The word "failure," in the technical sense, implies that there was, or should have been, an ability to avoid the failure, and I don't think we have enough facts. I certainly don't as, really, a private citizen reading newspapers to give you an opinion on that.

With respect to what we do here on out, I think it's going to be a function of intelligence, it's going to be a function of interdiction, going over to where we have to go over—whatever sanctuaries, as Ms. Hill mentioned—and do what has to be done there to destroy command and control capability and also to exploit intelligence. It means infiltration.

If one of those 19 hijackers had spoken—maybe they did, maybe we don't know about it yet—incautiously or imprudently to someone in some place where that information could have been captured, we could have had a day of terror prevented instead of September 11. There's all kinds of possibilities there.

So infiltration. We need to have our agents sitting around wherever they were sitting around in Hamburg and the UAE and other places, as well as in the caves over in Afghanistan so we can know what is going on. All those factors, I think you know, working together, have to occur.

But as you just asked the question—or somebody—Mr. LaHood just asked the question, you know we shouldn't—this is a hard thing to say, I guess, but we should not give the mistaken impression to people listening to our debate here that, you know, there's a secret formula for preventing this: If we could just reorganize homeland security; if we could just give a couple of billion dollars

to the FBI; if we could just do a little bit better, we're going to prevent these things.

That's a fallacy, and it's a misleading impression. If that was possible, we wouldn't see any attacks in Israel, with their experience and expertise and skill.

So we have to, unfortunately, accept the reality that these attacks from time to time, even on a spectacular and shocking and horrific basis, will succeed. Our job is to reduce those incidents, to make those attacks as unlikely and infrequent as possible. But it's not just a question of rearranging the chairs on the deck.

Mr. ROEMER. As I at least meant to say in my opening statement, I don't see this as a smoking gun. I don't see a national failure, meaning it could have been prevented. I think mistakes and gaps and failures and disconnects were out there. I'm not sure that this committee has found or will find a smoking gun. We sure need to correct the mistakes and gaps and disconnects.

Ms. White, what would you say about that?

Ms. WHITE. I certainly think we need to have—zero tolerance is an overused phrase, but we have to have zero tolerance for any instances of failure to communicate, whether it's between the FBI and CIA or whoever. There's no silver bullet; I think everyone agrees on that.

We are more vigilant now. I think everyone has lowered the bar—I'm talking about the cops on the beat, as well as FBI and CIA and everyone else—for what will have us take the next investigative step.

I think we have a list of things from all these cases we've done, and the investigations we've done, and the cooperating witnesses, you know, who have been debriefed—sort of their wish list of various terrorist attacks. And as apocryphal as they still may look in terms of the reality, we have to assume it could happen and figure out how best to anticipate that.

We're doing a lot of it in the way of homeland security, which I think is critical. Where we're most vulnerable, we need to shore ourselves up. We're way ahead of where we were, but we're still vulnerable.

Mr. ROEMER. Mr. Pillar.

Dr. PILLAR. I would just associate myself with everything Judge Freeh said in response to your question. It's all the things he mentioned and more.

On the question of preparing the American people, I would just underscore what I tried to say in my opening remarks: There is no silver bullet. We should not let the American people think that by this next set of changes or fixes, whatever they may include, somehow we've solved the problem.

I think we can learn some lessons from the Israelis in this, whose government has made conscious efforts to psychologically prepare their people for dealing with terrorism—not accepting it, but dealing with it in a way that tries to minimize the psychological impact that's an inherent part of what the terrorists are trying to do.

Chairman GOSS. Senator Roberts.

Senator ROBERTS. Thank you, Mr. Chairman.

Dr. Pillar, I am intrigued by your statement on page 3 when you said what is the lesson to be drawn from this episode, apart from the direct one that the Intelligence Community and the FBI were working closely with the relevant regulatory agency as early as the mid-1990s to call attention to the foreign terrorist threat to domestic civil aviation.

I think it has to do with how much our national willingness to respond with things like expensive new security measures depends on the reality of past tragedies, more than projections of threats that have not materialized.

Here's the key: The Intelligence Community has a duty here. As any new intelligence analyst is taught—and Kie Fallis can tell you about this—what matters is not just to make the correct deductions and hit the right notes, which may look good in postmortems, but to beat the drum loudly enough about impending threats to have some chance of making an impact on policy. Of course, if you beat it too loud, you get the drum around your head.

My question to all of you is, what keeps you up at night? What drum would you like to beat, if in fact you could beat one, to change policy, as opposed to what you have been doing within the confines of your jurisdictional responsibility?

Start with Ms. White.

Ms. WHITE. Get the walls down and make sure all the information is shared and analyzed real time by excellent expert analysts.

Judge FREEH. Going beyond the scope of my prior responsibilities and, I think, to the degree of certainty that we are able to identify a state, or state-class threat bent on destroying the United States and killing thousands and thousands of American.

Senator ROBERTS. Sanctuary, in other words?

Judge FREEH. Exactly. We have to make that decision. That's maybe the hardest decision that a President or a Congress has to make.

The circumstances have to be right. It takes enormous initiative and courage. But I think when we find that kind of a threat, we have to go after it and not relegate our response to subpoenas and search warrants.

Senator ROBERTS. So if Afghanistan was the sanctuary for al-Qa'ida, had we denied that sanctuary, we would have been miles ahead and, hopefully, something could have been done?

Judge FREEH. Miles ahead, and hopefully, we could have avoided some of the horror.

Senator ROBERTS. Paul, you're the drum beater—pardon me for calling you Paul, Dr. Pillar.

Dr. PILLAR. That's all right. What keeps me up at night, Senator, is in just the current group we're going after al-Qa'ida. But what comes after that? And what comes after that?

Senator ROBERTS. Hizbollah?

Dr. PILLAR. I am optimistic—terrorist groups including fragments of and successors to al-Qa'ida, even after we've reached a point we've beaten al-Qa'ida as an organization.

Senator ROBERTS. So we're at war with radical groups in the Islam world, Samuel P. Huntington.

Dr. PILLAR. I prefer not to use the term "war" with anyone in the Islamic world because of the connotations that that——

Senator ROBERTS. I said radical groups within the Islamic world.

Dr. PILLAR. Certainly with the radical groups. But again we should not make the mistake that we have our sights on one group or one state, and once we've eliminated that, we've gotten us through the——

Senator ROBERTS. So the Usama bin Ladin syndrome, if you get rid of him, you're okay.

Dr. PILLAR. I think that's—that's a mistake to say if we've gotten rid of him, it's okay. Look at the current situation where it's uncertain whether he's dead or alive. I think most of the analysts who follow the problem would agree, even if his dead body were to turn up tomorrow, we still have a serious problem with either the people who are in his organization now, or as I say, there will be numbers of fragments or successors to it.

Senator ROBERTS. Kie, you were a brave and successful drum beater. Do you have a drum that you would recommend that you could beat on now in terms of making a policy change?

Mr. FALLIS. Well, sir, I would just build on what Dr. Pillar said and that is the concern that I have over how these groups will evolve and change.

Beginning in 1998 is when you saw a major evolution in the capabilities of the al-Qa'ida network and their ability to target U.S. interests, I believe. And I think the evidence is there of another actor that helped these people gain this capability; and as their sanctuary has been denied to them in Afghanistan and they seek other places, other leaders under which to coalesce, that the results are potentially very dangerous for the U.S.

Senator ROBERTS. So a policy of preemption, no matter how tough it is—and it is very tough with changes in foreign policy, military tactics and the political situation—that's a road we have to take.

Mr. FALLIS. I believe so, sir. I think the static defense is always doomed to failure.

Senator ROBERTS. Thank you.

Chairman GOSS. Mr. Chairman.

Chairman GRAHAM. Thank you, Mr. Chairman. I have two areas that I'd like to question in.

One is, as I said in my opening statement several hours ago, I was concerned about the fact that we seem to have limited knowledge on some of the strategic issues relative to terrorist agents who are within the United States, including numbers, capabilities, intentions, relationships with headquarters organizations for purposes of command and control financing, general support.

Do you share my concern about our limited knowledge of those issues? Is that an important set of questions? And if it is important, how do we go about increasing our strategic knowledge of who our adversary is?

Judge FREEH. Well, I'll start, Mr. Chairman.

I think it is an important and valid concern. I mentioned before that—again, now more as an observer than a knowledgable insider—the huge increase in cases and identified subjects in the United States, people who fall into the category that you've just articulated a legitimate concern about, cases being opened and techniques and resources being expended that obviously were not being

expended before—my belief is that a lot of that information—at least this is what I'm told; in fact, I read it in the papers on Sunday—a lot of that information is from exploited intelligence received overseas by the very military action that we've all talked about today as, in some cases, the only alternative to, you know, what we can do in a passive way to deal with this problem.

So I think, you know, that kind of exploitation of intelligence translated into active surveillance and investigations and collection, which leads to detentions, immigration violations, jaywalking, whatever the case may be to neutralize that threat has to be done.

But I think the intelligence has to come from someplace. We can't come up with an invalid profile or stereotype, and that becomes the focus of what we do.

We don't do that in America. We don't do it well, and we don't do it at all. I think it has to be done on the basis of information and intelligence. And you get that inside the country by informants and infiltration. You get it outside the country by exploiting the things that are being exploited.

That's where the focus, I think, needs to be.

Chairman GRAHAM. As an example, someone has characterized the al-Qa'ida as being almost Germanic in their obsession with record-keeping and, thus, the large volumes of materials that we're getting; and that among those records maybe we have, we hope we'll have, things like rosters of students who attended these training camps and thus, put ourselves in a position to begin to ask the question, Are some of these students who were trained in specific skills while they were in Afghanistan, do we have any reason to believe through visa records or immigration records or others that they might be in the United States today?

Is it your sense that we are, to use your term, "exploiting" some of the data that we're now gathering through interrogations and document seizures in Afghanistan and elsewhere?

Judge FREEH. Yes it, is. That's exactly what we're doing. And to go back to the other point made here several times, Mr. Pillar most recently, the importance of our overseas liaison and contacts to the extent that our counterparts, whether they be police officers or security services, in dozens and dozens of countries are willing to impart that information to us, that they trust us enough that they will give us access to that kind of information.

That's the basis upon which leads and prevention, you know, translates into homeland security.

Chairman GRAHAM. Thank you.

Chairman GOSS. Ms. Pelosi.

Ms. PELOSI. Thank you, Mr. Chairman.

Following up on the Chairman's line of questioning, I want to refer to something in your testimony, Judge Freeh. You said, in 1996 the Khobar bombing investigation demonstrates the FBI's successes and limitations in combating foreign-based terrorists who wage war against the United States.

For us at the committee and for all of us involved in intelligence in any way, force protection is our highest priority, and certainly pre- and post-September 11 forces overseas and in our own country. It was interesting to me that we had troops in Saudi Arabia. When I read in your testimony, I was surprised to read that it said,

because of the FBI's prior contacts with the Saudi police service, the Mahabeth, and the Interior Ministry, that had been carried on from offices in Rome and, later, Cairo; the FBI lacked any effective liaison or relationship with its counterpart agency in Riyadh.

It seems to me that the minute we put troops on the ground, part of that arrangement should be that there would be an FBI presence in the country. And it doesn't have to be highly visible. But this terrible tragedy which—before we got over it, we were into East Africa; and before we got over that, we were in the *Cole*; and then, of course, September 11—this terrible tragedy of losing our young people in the armed services—you had to come from the United States, send scores of agents there to investigate, to do the forensic work, et cetera, at the scene. Wouldn't you think that it would be, or would you recommend that the minute we put troops on the ground there's an FBI presence—visible or not—in the country, and that be part of the arrangement?

Judge FREEH. Yes, I would. But maybe—going beyond that, it may be more significantly—you know, those are relationships that have to be grown over a period of time. When the bombing took place at Dhahran, the liaison between the FBI and the Saudi police was out of Rome. You know, every two years, the agent would come by and talk to somebody, and that was it; there was no high-level counterpart interaction. We didn't know who to call. They didn't know who to call, to the extent they wanted to work with us.

Ms. PELOSI. I find that appalling. We have troops on the ground, they're a target, we can imagine that they would be a target, and yet we don't have—we have somebody in Rome who stops by every now and then.

Judge FREEH. I couldn't agree with you more.

But just to finish my sentence, the notion is getting those people on the ground before the troops are there.

Ms. PELOSI. Of course.

Also you go on to talk about the cooperation the FBI received as a result of Prince Bandar and Nayef's personal intervention and support was unprecedented and invaluable. From time to time a roadblock or legal obstacle would occur, which was expected given our marked differences. Despite these challenges, the problems were always solved by the personal intervention of Prince Bandar and his consistent support for the FBI.

I would certainly hope that while we cannot get there before the troops get there, where they are now, that we would move quickly to make sure we have a presence, the liaison relationships established, in any of these countries; and certainly before we send troops to any new country for any duration as a presence that we would do that.

Judge White mentioned in her comments—just in passing, she said, the value of the cooperation that we have—let's see—we hold on to the coalition that we have in the fight against the war on terrorism, so that we can share information and how valuable that is. And it seems to me that it would be more valuable, the stronger the presence.

Judge White, would you like to speak to that?

Ms. WHITE. The single most important thing—I guess there are several single most important things that we have talked about,

but I think in the war on terrorism, our ability to combat it, protect ourselves, is by holding on to this world coalition and expanding it; because if you have a hole in it, that's where the next plot is going to come from. That's where the next sanctuary is going to be.

And to the extent Director Freeh just did an amazing job at globalizing the FBI, which is making possible that coalition now, in my view—I mean, it's not—we don't have everybody in it; we need to get everybody in it. And the FBI doing the groundwork for that "everybody" is where I think it is critical.

Ms. PELOSI. I thank you.

Judge Freeh, I was not saying that you should have had it done. I think this is something at the State Department, at the National Security Council level that has to be part of the package, before we put our—or as we put our troops on the ground, or as you said we do. So I commend you for your work.

But I think that there needs to be some higher level—well, we all look to a higher level in terms of the Federal Government, to the executive branch, making sure that this happens before we go on.

Thank you all. Thank you, Mr. Chairman.

Chairman GOSS. Senator Shelby.

Vice Chairman SHELBY. Thank you, Mr. Chairman.

I want to go back to basically the analytical center, you know, where—fusion center or wherever you want to talk about.

Judge Freeh, you talk about, reading an excerpt again from your remarks—I'll quote you, and you correct me if I'm wrong here in the quote, or if the quote is wrong—you say, "It's very important in hindsight to segregate this relevant information and put it into a dedicated time line"—I agree with that—"as we do in a post-mortem."

But isn't it very important to put all this information together, relevant information, fusion center, to try to predict something; in other words, try to discern something is going to happen, just as well?

Judge FREEH. Absolutely. Prevention is what the priority is and has to be in this area, and the prevention is only as good as the success of that fusion and its predictability.

Vice Chairman SHELBY. If we don't put together—that is, all of us collectively, the Congress, the administration—and put the resources that we keep talking about together for some type of a fusion center, we'll pay again, will we not?

Judge FREEH. I agree 100 percent.

Ms. WHITE. Definitely agree.

Dr. PILLAR. Yes, sir.

Mr. FALLIS. Yes, sir.

Vice Chairman SHELBY. Judge Freeh, I believe you said today that the FBI—you're speaking of the Bureau—was intensely focused on an attack within the U.S. Dale Watson, who has just retired from the FBI and was head of the FBI's counterterrorism program under you and under Director Mueller, told the staff he was, "98 percent sure the attack would be overseas." He's head of the FBI's Counterterrorism Center. And this was based upon the summer of 2001 increase in the chattering threat warnings that were put over the air.

Is your view basically inconsistent with Mr. Watson, who was head of your Counterterrorism Center?

Judge FREEH. I don't think it's inconsistent.

Now, I'm not privy to the summer information——

Vice Chairman SHELBY. Sure, you'd left.

Judge FREEH. What I will tell you is, when I did leave, which was in June——

Vice Chairman SHELBY. When you left, you meant you retired.

Judge FREEH. I'm sorry. When I retired, I was, as I said, working and conscious of that line of events and activities going back to the Lower Manhattan attack on the Trade Tower in February of 1993. Ressam confirmed that we were being targeted within the United States, and it was a miss that we were lucky to have avoided, but the intent was still to attack us in the United States.

The fact that he was expecting, by the end of the summer, an attack overseas I don't think is inconsistent with the fact that we were also intensely focused on the targeting of targets within the United States. I don't think that's inconsistent.

I don't know what information he had at the end of the summer which I don't have.

Vice Chairman SHELBY. It's my understanding that—and this is coming from a December, 2000, report that the FBI and the FAA published. It was a classified assessment—and I'm not going to read from that—that suggested concern about the threat to domestic aviation, but basically saying that the FBI investigations or judgments confirmed domestic international terrorist groups operating in the U.S., but do not suggest evidence of plans to target domestic civil aviation. In other words, the FAA basically told us that at no time did the FBI or the CIA tell them or warn them about the possibility of airplanes being used as weapons in this terrorist war.

Judge FREEH. Well, I'm not privy to that report. I'm also not trying to avoid your question. I'm not aware of any dissemination, while I was in the FBI, to the FAA that airplanes would be used, or could be used, as suicide weapons, as they were. I am aware not just from the Gore Commission, but just from being alive that airplanes and hijackings of airplanes have been a premier terrorist target and activity for the last 25 years. And that should come as no shock to anybody.

Vice Chairman SHELBY. I can read this. I was just told by staff it is unclassified—we have to be careful in what we read up here—and I'll read this from this report, just for the record.

It says—in a December, 2000, report, the FBI and the FAA again published an assessment that suggested less concern about the threat to domestic aviation. "FBI investigations confirmed domestic and international terrorist groups operating within the U.S., but do not suggest evidence of plans to target domestic civil aviation. Terrorist activity, when in the U.S., has focused primarily on fundraising, recruiting new members and disseminating propaganda. While international terrorists have conducted attacks on U.S. soil, these acts represent anomalies in their traditional targeting which focuses on U.S. interests overseas."

Gosh, it was so wrong, we know now. Do you agree with that?

Judge FREEH. Well, you know, "evidence" is a very technical and a very significant word. I don't know what they meant to communicate when they said "evidence" as opposed to the "threat." Just repeating my last answer, hijacking of aircraft up to and including September of last year was always considered by everybody as a primary target for a terrorist, which is why the efforts were taken to fortify airports and profiling and security. You know, that should come as no surprise.

Vice Chairman SHELBY. Should it have come as any surprise that airplanes would be used as weapons to crash into the Trade Towers considering that in 1995—the Filipino situation that I know you're familiar with, you know what happened there, and the information, the French scenario where someone was apprehended, and they had information they were going to use that plane to crash into, I believe, the Eiffel Tower, and other information. Should it have come as a surprise?

Judge FREEH. The answer is no. But you've just very expertly distinguished what we call the strategic intelligence from the tactical intelligence.

Did the FAA and the industry have that strategic intelligence? They probably did. Did they have the tactical intelligence? Did anybody have the tactical intelligence that aircraft would be used in the manner that was used on September 11? I think the answer to that is no.

That's where the committee and the commission needs to get into the weeds.

Vice Chairman SHELBY. Thank you.

Thank you, Mr. Chairman.

Chairman GOSS. Thank you very much. The final question that I had went to frustration that I have felt, and I'm sure you have all felt too in the positions of responsibility that you've had.

I don't think, as I look at this panel of very distinguished and experienced people who have been working with this problem on behalf of the United States of America—writing about it, dealing with the intricacies of it and the complexities of it—that there is any doubt at all after the hearing today that we understood pretty well what the problem was.

And I don't think there's any doubt at all from my working association with people at the table, and the reputations and the accomplishments that they've made, that they had excellent ideas on how to take care of weaknesses in the system or problem areas; or where resources were short, bring attention to those underinvestments.

My question is that we have seen a lot of similar witnesses who have shared in the work product here with us, trying to get to the bottom of all of this and how we can do better.

How is it, do you think, that all of the expertise and all of the authority that was embodied in articulate, knowledgeable, hard-working people failed to receive the audience that it should have gained so that we could have focused our resources, our country, our constituents?

I guess what I'm asking is, how come nobody was listening? Do you have any idea how we can do better on sounding the trumpet when we see these things happening to us? Because I think we've

all admitted we were surprised at what happened, how it happened, but we weren't surprised that it happened.

Ms. WHITE. I think that September 11 was that trumpet. And I think, unfortunately and tragically, but perhaps understandably, it took tragedy, horror at that level, to grip certainly the public's attention on this.

And I think, to some extent—I mean, look how we've had to change our lives already within this country and around the world. That's not something we do lightly, or want to do lightly either, absent, you know, an attack of that scale.

The East Africa bombing case, 24 people died over in East Africa. We tried the case in the Southern District of New York in Lower Manhattan. Wrenching testimony, but still, I think, within the country, that's "over there," and when it was "over there," it didn't grip in the same way.

So I think it's gripping now.

We don't want to, you know, lose sight of the fact that it's a clear, present and continuing danger, though. So I think we still have to be trumpeting, but I think September 11 was a loud call.

Chairman GOSS. I hope you're not sentencing us to becoming a reactive society when I think we need to be a visionary society. Perhaps that's one of our lessons.

Judge Freeh.

Judge FREEH. I share your frustration, Mr. Chairman. And, you know, I hope September 11 is the trumpet. I just don't know.

I mean, you know, did the United States and the same class of wonderful people that you just described, you know, know in 1941 that Japan was capable of attacking the United States? Yes. Was anything done at the time to build up our military?

Did the world know by the summer of 1933 that the National Socialists in Germany were going to try to take over the world and murder six million Jews? Sure, they did. And they sat around at the Evian Conference, 32 nations, and couldn't come up with a solution.

So, you know, are we doomed to this kind of failure? You know, I hope not. I hope September 11 has sounded that trumpet. But it's going to be up to not just the leadership of the country, but really the people to keep that vision.

I think you used the word completely correctly in front of us. And our experience in these things is not good as human beings and as Americans.

Dr. PILLAR. Mr. Chairman, the event last September clearly was a trumpet. The question is how quickly and how deeply the blare of that trumpet will fade over time. I think it's already fading some. You've seen this consistent pattern throughout this period, this last decade that this hearing has been devoted to, of a spike-up in interest and concern when we have a major incident; and then the line of concern and interest in this topic goes down.

Clearly, the spike on September 11 was far greater simply because of the enormity of the act. But it, too, is already a curve coming down. And the one piece of advice I would give to political leaders like yourself is to try to spread out your action and rhetoric and legislation and everything else, so it's not all bunched up right after each attack, but continue to remind the American people,

along with the rest of us and the press and those of us who write books and so on, to get the point across that the things that we need to do in this counterterrorist business cannot all be sandwiched in the first two months after each major attack. It's got to be consistent.

Chairman GOSS. My time has expired, but I do want to pass along a question to each of you. It's a yes-or-no question that some of my colleagues are passing along to me these days.

It is, do you think we are overreacting to 9/11 as a Nation?

Ms. WHITE. No.

Judge FREEH. No.

Dr. PILLAR. No.

Mr. FALLIS. No.

Chairman GOSS. Thank you very much.

Chairman Graham.

Chairman GRAHAM. Can I ask a question which is in the same line of the Chairman's questions?

Is there anybody in the world who is doing the intelligence business better than we are, that we could learn some lessons from? Particularly in this area of what I call the revitalization, or the reinvention, of agencies as circumstances change, and the need to alter behavior in order to respond to the new circumstances, are there any role models that we should be garnering lessons from?

Dr. PILLAR. I can't think of any one role model, Mr. Chairman, but there are a lot of little lessons to be learned with regard to going after particular types of groups.

In many cases, we have foreign counterparts that have been on the front line literally in the sense of their interest and their citizens being the victims of attacks by a particular group; and so they know a lot more about that group and how to go after that group and how to collect against that group than we do.

And so you can look at those sorts of group-specific, region-specific lessons. But, no, sir, I can't think of any one role model that is the one we need to emulate on everything. We need to learn lessons from a lot of different partners.

Chairman GRAHAM. Thank you, Mr. Chairman.

Chairman GOSS. I want to thank you. Not only do I admire your wisdom, but I admire your stamina. And I really admire anybody who can sit for this many hours. We have the opportunity to get up and walk around.

I will close this hearing by saying, the committee will meet in closed session tomorrow, October 9, at 2:00 p.m. in S–407 in the Capitol.

The committee will again meet in open session on Thursday, October 10, at 10:00 a.m. in this room. On Thursday, our witnesses will be the Director of Central Intelligence, Mr. George Tenet; the Director of the Federal Bureau of Investigation, Mr. Robert Mueller; and the Director of the National Security Agency, General Michael Hayden. The Directors have been requested to address, among other matters, the issues that have been raised and recommendations made during the course of our 20 open and closed hearings.

And I would say today we have covered an awful lot of material that has been extremely helpful to us and, I hope, to the American

people—understanding what an amazing group of hard-working people we have out doing the business of America's national security in a number of fields, where it all has to be done, and we seldom pay it any attention.

So I thank you all. Godspeed in your work.

Chairman GRAHAM. I would like to join in those words of our Chairman and express my appreciation for the very excellent insights and the sharing of your depth of experience. We appreciate it. We've taken it on board; I hope we can use it properly. Thank you.

Chairman GOSS. Thank you all.

[Whereupon, at 5:00 p.m., the Joint Inquiry Committee was adjourned.]

Proposals for Intelligence Reorganization (1990-present)

1992: Boren-McCurdy

- Major legislative initiative by House and Senate intelligence committee chairmen to restructure intelligence community;
- Created a Director of National Intelligence (DNI) with authority over all IC programs and resources, including those within the DOD;
- Created two Deputy Directors of National Intelligence—one for analysis and estimates and one for IC affairs;
- Created a separate Director of CIA;
- Consolidated analytical and estimated efforts throughout the IC into a separate office under one of the Deputy DNIs;
- Created a National Imagery Agency within the DOD;
- Authorized the Director of DIA to task defense intelligence agencies and shift resources among them;
- Legislation was not adopted—defeat was credited to strong opposition from DOD and the armed services committees.

1995-1996: Commission on the Roles and Capabilities of the U.S. Intelligence Community (Aspin-Brown Commission)

Key Recommendations:

- Create a two-tier structure to carry out the institutional role of the National Security Council (NSC) comprising a Committee on Foreign Intelligence (chaired by the Assistant to the President for National Security Affairs and including the DCI, Deputy SECDEF, and Deputy SECSTATE) and a subordinate Consumers Committee to provide guidance for priorities and to evaluate performance.
- Replace the position of Deputy DCI with two new deputies—one for the Intelligence Community and one to manage the CIA who would be appointed to a fixed term of six years.
- Dual hat the directors of NSA and NIMA as Assistant Directors of Central Intelligence for signals intelligence and imagery, respectively, with the DCI concurring in their appointments and providing performance evaluation input to the SECDEF.
- Realign the intelligence budget into "disciplines" which are then coordinated by "discipline managers," for example the Director of NSA would be the discipline manager for all activities related to signals intelligence.
- Restructure the National Intelligence Council, which prepares intelligence estimates, into a more broadly based National Assessment Center under the DCI but outside of the CIA.
- The Director for Intelligence (J-2) currently assigned to the DIA should be constituted as part of the Joint Staff.

- A single focal point should be created on the staff of the SECDEF to coordinate how strategic and tactical intelligence is provided to the field commanders.
- Transfer all responsibilities of the Defense HUMINT Service to the CIA to include military personnel on detail from the DOD as necessary.
- Preserve the NRO as a separate agency and ease licensing restrictions on commercial imaging systems for foreign sale in order to encourage greater investment by U.S. firms in such systems.

1996: IC21: The Intelligence Community in the 21st Century (HPSCI Staff Study)

Key Recommendations:

- Give the DCI a stronger voice in the appointment of directors of intelligence agencies under the DOD.
- Re-establish a Committee on Foreign Intelligence (comprising the Assistant to the President for National Security Affairs, the SECSTATE, SECDEF, Chairman JCS, DCI, and Attorney General) within the NSC to provide more regular policy guidance, feedback, and oversight.
- Appoint an additional Deputy DCI to manage the CIA.
- Consolidate and rationalize the management of infrastructure and services across the IC to include personnel management, training, security, and information systems.
- Designate the Director of DIA as the Director of Military Intelligence.
- Reinforce CIA's role as the premier all-source analytical agency by housing all analysts associated with all collection disciplines.
- Reinforce DIA's role as the focal point for management of Defense all-source analysis and production.
- Create a Clandestine Service comprising CIA/DO and DHS and place it under direct control of the DCI.
- Under the Deputy DCI for Community Management, create an organization responsible for all collection tasking.
- Consolidate technical collection activities (SIGINT, IMINT, MASINT) and first-tier exploitation into a single Technical Collection Agency.
- Consolidate Community R&D and acquisition of reconnaissance capabilities into a single Technology Development Office.
- Establish a National Intelligence Evaluation Council to evaluate IC-wide collection and production, and to interact closely with the requirements, collection management and resource functions of the Community Management Staff.
- The SECDEF should exercise his authority to create a separate Assistant Secretary of Defense for Intelligence, reporting directly to the Deputy SECDEF.

1997: Modernizing Intelligence: Structure and Change for the 21st Century (Odom Study)

Key Recommendations:

- Make no statutory changes to DCI's authority.
- Strengthen the role of the National Intelligence Council (NIC) in providing unique national-level analysis and overseeing analysis and production throughout the IC.
- Separate the Directorate of Intelligence from the CIA and subordinate it to the DCI through the NIC.
- Restructure the Community Management Staff (CMS) by creating five primary staff sections: Evaluation Management; Resource Management; Science and Technology; Counterintelligence Management; and Security Policy.
- Keep the Defense HUMINT Service (DHS) as a single DOD organization under the operational control of CIA/DO.
- Create an overt HUMINT organization in DOD.
- Put all DIA electronics intelligence collection under NSA and put its IMINT collection under NIMA.
- Abolish the NRO and transfer its program offices to NSA and NIMA.
- Create a formal J-2 intelligence organization on the Joint Staff for support to military operations.
- Designate the Director of DIA the coordinating manager of all military intelligence support.
- Designate the Director of NSA the national manager for SIGINT in charge of operational control and management of the entire system.
- Direct the DCI to use his CMS Science and Technology Office for an examination of NSA's core capabilities.
- Designate the Director of NIMA the national manager for imagery intelligence (IMINT).
- Restructure CIA by giving it two major components—the national clandestine service (NCS) and a component for handling overt HUMINT. Designate the Director of this restructured organization the national manager for HUMINT.
- Retain a residual Science and Technology capability for support to HUMINT.
- Allow the CIA/DO to retain its status at the covert action agency, but make it dependent on the DOD's capabilities for the conduct of any paramilitary operations.
- Create a National Counterintelligence Service (NCIS) with the FBI's CI department forming its core.
- Designate the Director of the NCIS as the national manager for CI responsible to the DCI.

2001: U.S. Commission on National Security (Hart-Rudman Commission)

Key Findings:

- The basic structure of the Intelligence Community does not require change.

JOINT COMMITTEE HEARING ON THE DIRECTOR OF CENTRAL INTELLIGENCE AND INTELLIGENCE COMMUNITY RESPONSE TO ISSUES AND RECOMMENDATIONS RAISED AT PREVIOUS HEARINGS IN REVIEW OF THE EVENTS OF SEPTEMBER 11, 2001

THURSDAY, OCTOBER 17, 2002

U.S. SENATE, SELECT COMMITTEE ON INTELLIGENCE, AND U.S. HOUSE OF REPRESENTATIVES, PERMANENT SELECT COMMITTEE ON INTELLIGENCE,

Washington, DC.

The Committees met, pursuant to notice, at 10:10 a.m., in Room 216, Hart Senate Office Building, the Honorable Bob Graham, Chairman of the Senate Select Committee on Intelligence, presiding.

Senate Select Committee on Intelligence Members Present: Senators Graham, Shelby, Levin, Feinstein, Wyden, Bayh, Kyl, Hatch, Roberts, DeWine, Thompson, and Lugar.

House Permanent Select Committee on Intelligence Members Present: Representatives Goss, Bereuter, Gibbons, Hoekstra, Burr, Pelosi, Harman, Condit, Roemer, Reyes, Boswell, and Peterson.

Chairman GRAHAM. I call the meeting to order.

This is the ninth public hearing of our inquiry into the events surrounding the terrorist attacks of September the 11. We have also held 13 closed sessions.

Under our current schedule, this will also be the last public hearing, and I would like to take this opportunity to thank the Members of the House and the Senate committees for their commitment to this very important process.

I am especially grateful for the cooperation of our co-chairman and my good friend, Representative Porter Goss, as well as the outstanding and cooperative relationships with Congresswoman Nancy Pelosi and my Senate colleague, Richard Shelby.

I would also like to express my personal gratitude for the outstanding work of our exceptional staff of investigators led by Ms. Eleanor Hill. We will hear another presentation from Ms. Hill in just a few opening statements.

As we contemplate our next step in this inquiry, the writing of our final report, I would like to say how important I believe the experience of conducting this inquiry in a joint manner, the first time in the history of the Congress that such an enterprise has been undertaken, will be to our final report.

The value will be that, when we make our recommendations for reform, both House and Senate Members will do so having heard the same testimony, shared the same information, listened to the same discussions. Based on that, we will make our recommendations. These recommendations will be the most important legacy of our hearings, launching reforms that will assure the American people that our first line of defense against terrorism, our intelligence agencies, are doing all that they can to detect, deter and disrupt schemes against our homeland and American interests abroad.

As we heard at our last public hearing on October 8, there have been a succession of reports recommending reforms to the Intelligence Community. A majority of those were issued prior to September 11, 2001.

What most of those reports had in common, sad to say, is that relatively little has been adopted from them. I am hopeful that, as a result of this joint process, our recommendations will be taken more seriously and will have a greater impact on the Intelligence Community in the 21st century. I look forward to working with all the members of the House and Senate committees on these recommendations in the weeks to come.

Today's hearing will be in two parts. First, we will hear from Ms. Eleanor Hill, who will review the major issues that have been identified in the course of the inquiry. We will then hear from a panel of distinguished witnesses consisting of the Director of Central Intelligence, the Director of the Federal Bureau of Investigation and the Director of the National Security Agency.

Among the questions that we look forward to exploring today is what the Intelligence Community in general and the CIA, FBI and NSA in particular have learned from September 11 regarding what should be done to improve our counterterrorism programs; and, in addition to learning what should be done, what are they actually doing and planning to do in order to improve the effectiveness of their programs.

We will also discuss with our witnesses what the President and the Congress should do to assist them in these reforms.

I'll now ask my colleagues, starting with Congressman Goss and then Vice Chairman Shelby and Ranking Member Pelosi, if they have any opening comments for today. Chairman Goss.

Chairman GOSS. Thank you very much, Chairman Graham. I just wanted to add briefly a couple of points to the very kind opening remarks you've made.

I think that these public hearings have been a very helpful window into the Intelligence Community to help Americans appreciate a little better the men and women and the extraordinarily tough jobs that they do for our national security, and I think for that it has been extremely helpful as a sidebar to our other stated mission.

I think trying for all of us—trying to understand terrorism better and how we must fight it is something of a national challenge, and I think these public hearings have been very useful in awareness and alertness areas.

I am very grateful for the participation of the Members. I believe that everybody has participated fully and gotten involved and done their homework and asked questions and been very much a part

of this, which was our hope from the beginning, as you know; and I do take away from this that there is a possibility of a happy marriage between the Senate and the House, which will inevitably have some bad days, but I think that it is reassuring to the American public that, in fact, we do work together.

There is a part of this that the American public has not seen. It is what is going on behind the scenes which we can't talk about entirely because of the protection of sources and methods and plans and intentions and matters that deserve to be held closely at this time because of ongoing investigations and other legitimate reasons. In time, those will be revealed as well for the most part, I suspect, as is usually the case.

So, in many ways, this is openers, what we're doing; and there will be follow-on. We all know that, and we think that we have created a springboard for that. And the rest of the work that our staff has done under very able leadership of Eleanor Hill is I think remarkable and will serve those who come after us in this process very well.

I think it is very clear that our oversight work for these two committees in the future is going to be very vigorous and very required; and when Ms. Hill makes her remarks this morning, which I've had the privilege of seeing, I think it is an excellent blueprint of the problem, some of the solutions that might be out there, and some of the places we're going to have to direct our attention. So I urge people to pay attention to her statement this morning.

I will also point out it is obviously not just intelligence oversight. It is going to be oversight of many of the committees of Congress as well. So I think we have served not only our purposes in the narrow area of our responsibilities for intelligence but a broader picture for the responsibilities of Congress to try and understand better the events of 9/11.

Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Congressman Goss.

Senator Shelby.

Vice Chairman SHELBY. Thank you, Mr. Chairman.

First of all, Mr. Chairman, I want to thank you for your kind personal remarks. I've served with you when you were the Vice Chairman, as I am now, and when I was the Chairman; and I'm serving now as your Vice Chairman and you're the Chairman. I prefer to be the Chairman, but I've enjoyed working with you as the Vice Chairman.

Having said this, Mr. Chairman, this is probably our last public meeting together, the two of us, and other members of this committee. And while this may be our last public hearing before the Congress adjourns, too, for the year, I believe it is important to point out, Mr. Chairman, that our work will continue until the 107th Congress comes to an end.

We will continue to ask questions and review documents until we're compelled by the calendar to conclude the fact-finding phase of this inquiry. We will then begin the process of drafting a report. I'm hopeful, Mr. Chairman, that we will reach a consensus, but I'm also cognizant of the difficulty of such an undertaking.

Mr. Chairman, while our work will ultimately end, the process that we have begun must not. If we've learned anything here, it is

that nearly every day brings a new revelation, a new bit of information or a new line of inquiry. That, Mr. Chairman, is why the leadership of these committees have determined that a commission must be established to continue and to expand upon the work that we are doing here.

I believe, Mr. Chairman, the American people should know that we've been limited by time here, by resources, and, yes, by scope. We have been at work for a little over 6 months with a small staff examining only the performance of our Intelligence Community. The story of 9/11 and our inability to detect and prevent it extends far beyond, I believe, our intelligence agencies. The American people, Mr. Chairman, must know that the full story is yet to be told.

Mr. Chairman, we've learned many lessons, but there are many yet to be learned. We've answered many questions, but there are many yet to be answered. I believe our work has been useful and constructive in this joint inquiry. We've discovered many instances where our intelligence agencies failed to perform as we expect them to. We've also discovered, Mr. Chairman, many more examples of dedicated and tireless Americans performing their duties with distinction and honor. The American people should know that the latter is the rule, not the exception.

Often I hear commentators refer to our work as an effort to discover what caused the events of September 11. I think we can report safely to the American people that we have no doubt what caused 9/11. It was the twisted actions of a network of murders dedicated to killing Americans. What these committees are endeavoring to determine is why we were unable to detect and to stop this plot. That work is ongoing and I believe must continue if we are to ensure that this never happens again.

Mr. Chairman, I look forward to today's testimony, but I do so knowing full well that this is not the end of our work or the work that must still be done for the American people.

Thank you.

Chairman GRAHAM. Thank you, Senator Shelby.

Congresswoman Pelosi.

Ms. PELOSI. Thank you very much, Mr. Chairman.

I want to join in commending you and Mr. Goss for your leadership as chairmen of this joint inquiry since the beginning of this year. I think it provides a model for how we can work not only, Mr. Chairman, in a bicameral way but in a bipartisan way for the benefit of the American people. But the American people were well served by the two of you in the chairmanship roles, and I know that Mr. Shelby said that he would rather have been chairman, and I associate myself with those remarks.

In any event, when we came together to announce this joint inquiry, our statement of intent said and in our preamble we said to reduce the risk of future terrorist attacks, to honor the memory of the victims of the September 11 terrorist attacks by cutting a thorough search for answers to the many questions that their families and many Americans have raised, and to lay a basis for assessing the accountability of institutions and officials of government. I believe that included the Congress of the United States. The Senate Select Committee on Intelligence and the House Permanent Select

Committee on Intelligence adopt the scope of joint inquiry that we pursued.

Before I go into how I think that we have honored that charge, I want to join in—I want to say to Director Mueller, who I know—I hope is within earshot as we welcome our distinguished witnesses today, I want to express my condolences and those of all whom I work with for the loss suffered by the men and women of the FBI in the loss of their colleague in the tragic events of Monday night. The murder of Linda Franklin is another reminder that dealing with acts intended to instill fear, regardless of whether the individual or group committing them has routes at home or abroad, is our greatest security challenge. I hope that the Director will convey the condolences of our joint inquiry committee to his colleagues.

Four months ago, we began the hearings phase of our joint inquiry with these same witnesses in closed session. Since that time, we have been very well served by Ms. Hill and her Deputy, Rick Cinquegrana, and the joint inquiry staff. I think that—well, I'll say more about that later.

Although it was necessary to take much of the testimony on the September 11 attacks in secret, it was clear that there was a portion of the story that could be and in fact had to be made public. Through the open hearings of the past 4 weeks, that part of the story has been told. I want to commend our Staff Director again, Eleanor Hill; her Deputy, Rick Cinquegrana, and the joint inquiry staff for the effort that has gone into these public hearings. In my judgment, they have contributed significantly to increasing the understanding of the American people about the events that led up to the attacks.

As the hearings have made clear with respect to at least some of the hijackers, their associates and people who may have been their associates, signs were missed, opportunities were not seized and legal procedures were misunderstood. Had those mistakes not been made, would the outcome of September 11 been any different? We will never know. Perfection is a difficult standard to which to be held. With respect to counterterrorism activities, however, it is the only one that can apply. If not is something that can be reasonably attained then is something that must always be the goal.

Our witnesses have had the difficult job of trying to explain the unexplainable. It is not enough to say that we did not have enough money or enough people. No one does. It is always the case. It is about accomplishing priorities. It is about deciding what is most important from a host of important requirements and ensuring that, from available resources, those sufficient to do the job are assigned to it.

It is about recognizing where improvements are needed in ways in which business is done and making them, and it is about making certain that information that appears insignificant to one agency is shared as widely as possible with others on the chance that it has an importance beyond what is apparent on the surface.

One of our chief objectives, as was mentioned in our preamble, in this inquiry has been to making the American people safer than they were on September 11. Our witnesses today have a chance to describe how things have changed in the past year, how agencies are working more closely together and how the cooperative efforts

of the international antiterrorism coalition have contributed to successes against al-Qa'ida. I hope they will advise us whether our chances of preventing another attack on the United States are any better today than they were last September, and if not, why not.

I look forward to their testimony and agree with some of the comments of Mr. Shelby that, while we focused on the Intelligence Community mostly in this, that some of the answers go well beyond this, and we have to seek the truth wherever it is. I think that speaks to the need for an independent commission to build on the very excellent work that this committee—this joint inquiry has already produced.

With that, I commend the two distinguished chairmen once again and say that it has been an honor to be associated with their leadership and their work in this regard as well as that of Mr. Shelby, and I think he is perfectly appropriate in the role that he has now. Thank you very much, Mr. Chairman.

Chairman GRAHAM. Thank you very much, Congresswoman Pelosi.

Before hearing from Ms. Hill and our witnesses, I would like to present several administrative matters to the committees for consideration and action. At several earlier hearings, we have provided for supplementation of the record. We have done this without objection. As we prepare to bring our hearings to a conclusion, it would be desirable to extend that authority to supplement to our hearing record on a general basis. Accordingly, I ask unanimous consent that, one, classified staff statements be placed in the classified portion of the hearing record where appropriate. Is there objection?

Without objection, so ordered.

Two, that Chairman Goss and I, acting jointly after consultation with Ranking Member Pelosi and Vice Chairman Shelby, be authorized to place in our hearing record classified and unclassified exhibits that are designated for inclusion by any member of the two committees or by the Staff Director of the joint inquiry. Is there objection?

Without objection, so ordered.

Third, our practice throughout these hearings has been to invite witnesses by a joint invitation of the two chairmen, vice chairman Shelby and Ranking Member Pelosi. In the event that we determine that the full record of the proceedings should be amplified by additional witness statements for the record, I ask unanimous consent that the four of us acting jointly be authorized to invite and place in the record written statements by additional governmental or private organizations or persons. Is there an objection?

Hearing none, it is so ordered.

Finally, on June 18 the committee heard testimony in a closed session from the Director of Central Intelligence, the Director of the Federal Bureau of Investigation and the Director of the National Security Agency about what the Intelligence Community now knows about the September 11 plot. We then asked the Directors to declassify their testimony to the extent consistent with national security.

The Director of the FBI has previously submitted his declassified statement which was then included in our open record. The Director of Central Intelligence has now submitted his declassified state-

ment for the record. I ask unanimous consent that his declassified statement also be made part of the open record of these proceedings. Is there objection?

Hearing none, so ordered.

[The June 18, 2002, declassified statement of George J. Tenet follows:]

Final Draft 9-11 Testimony
For the DCI
Joint Inquiry Hearing
18 June 2002

Before Director Mueller and I focus on the 9/11 plot, as you've asked us to do Mr. Chairman, I would like to begin with some remarks on the context in which the attacks occurred. There are two key points:

- First, we had followed Bin Laden for many years and had no doubt that he intended a major attack.

- Second, the eighteen months prior to 9/11 were a period of intense CIA/FBI efforts to thwart dramatically heightened UBL operational activity.

We first locked onto Bin Laden in the period from 1991 to 1996 when he was in Sudan.

- During those years, he was principally a financier of terrorist attacks and our efforts against him competed with other deadly threats, such as those posed by Hizbollah – which at that point was responsible for the deaths of more Americans than any other terrorist organization.

- Bin Laden jumped right to the top of our list with his move to Afghanistan in 1996 and his drive to build the sanctuary that subsequently enabled his most spectacular attacks. This focus resulted in the establishment within CTC of a Bin Ladin-dedicated Issue Station staffed by CIA, FBI, DOD, and NSA officers.

- Bin Laden showed his hand clearly that year when he said that the June bombing of Khobar towers marked the beginning of the war between Muslims and the United States.

- Two years later, he issued a fatwa stating that all Muslims have a religious duty "to kill Americans and their allies, both civilian and military worldwide".

- He then attacked our East African embassies in 1998 and said that an attack *in* the US was his highest priority.

- We took this as his unequivocal declaration of war, and we in turn declared war on him, inaugurating an intensive period of counterterrorist activity that filled the months running up to 9/11.

There were three broad phases in that struggle before 9/11 and I want to set the stage for the 9/11 plot by telling you about them:

- *First, the pre-Millenium Period in late 1999.* UBL operatives planned a series of attacks against US and allied targets designed to exploit the millennium celebrations planned around the world. CIA and FBI worked closely and successfully to defeat these terrorist plans. We acquired information that enabled us to break up a large terrorist cell in Jordan that had been planning to blow up the Radisson Hotel, holy sites, and Israeli tour buses, and that had plans to use chemical weapons. The arrest of Ahmed Ressam coming across the Canadian border into the US was the single most compelling piece of evidence we had that UBL was intending to strike at us in the United States. During this period, we identified numerous terrorist suspects around the world and carried out disruption activities against more than half of these individuals including arrests, renditions, detentions, and interrogations.

- *Second, the Ramadan Period.* In November and December 2000, we had an increase in Ramadan-related threat reporting. Working with a number of foreign governments, we were able to successfully preempt attacks including a planned attack against US interests. Overall, these operations disrupted several al-Qa'ida plans and captured hundreds of pounds of explosives, as well as weapons, including anti-aircraft missiles. You will recall that the attack on the *USS Cole* had just occurred in October 2000, a serious defeat.

- *And finally, the Pre-9/11 Period.* Starting in the spring and continuing through the summer of 2001 we saw a significant increase in the level of threat reporting. Again, working with the FBI and foreign liaison services, we thwarted attacks against US facilities and persons in Europe and in the Middle East.

Thus, even before September 2001, we knew that we faced a foe that is committed, resilient and has operational depth. The Intelligence Community was already at war with al-Qaida.

- Few wars are a series of unbroken victories or defeats. We had had some successes and suffered some defeats—and we are finding things we could have done better.

- But we were already in action.

We had, in fact, considered ourselves at war with al-Qa'ida since 1998. By 1998, key elements of CIA's strategy were emphatically offensive rather than defensive. And in the spring of 1999, we put in place a new strategic operational plan whose central focus was to gain intelligence on Bin Ladin through penetrations of his

organization. This strategy structured our counterterrorist activity for the years leading up to the events of September 11.

- This strategy—which we called simply "the Plan"—as it evolved in conjunction with increased covert action authorities, was a multifaceted campaign against Bin Ladin and al-Qa'ida.

- The campaign involved a multifaceted program to capture and render Bin Ladin and his principal lieutenants. The range of operational initiatives employed included a strong and focused FI collection program using all means at our disposal to monitor Bin Ladin and his network around the world, and to disrupt al-Qa'ida operations.

- I do not plan to go into great detail on this campaign now—this hearing is about 9/11.

- But my message is that a full understanding of the events of 9/11 requires an understanding of this war in its entirety and, I hope subsequent hearings will develop the details of that story.

Now, with that as a backdrop, let me begin by characterizing the 9/11 plot in broad terms.

- First, the plot was **professionally conceived and executed**—it showed patience, thoughtfulness, and expertise.

- Second, it was **tightly compartmented**—we would have had to penetrate a very small circle of zealots to have learned the precise details of this plot ahead of time.

- Third, the plot was **resilient**—several blows to the operation occurred without derailing it.

- I'll amplify each of these points.

Start with what we know today of the **professionalism of the plot.** The 11 September operation was conducted carefully, patiently, and with evident understanding of how to operate in the United States.

- The hijackers--both pilots and others--entered the US at staggered intervals, from different countries, and through different US cities.

- We now know that al-Qa'ida leaders deliberately chose young men who had not carried out previous terrorist attacks and therefore would not have attracted the attention of intelligence services. Seventeen of the nineteen hijackers were in fact "clean," and the two hijackers who had an extensive

record of al-Qa'ida involvement--Nawaf al-Hazmi (#14) and Khalid al-Mihdhar (#12)--may have been added to the plot after it was launched. I'll return to this possibility later in my remarks.

- They also selected men from countries whose citizens traditionally have little trouble obtaining US entry visas and instructed them to travel under true name using genuine passports.

- The most important individuals in the plot--the pilots--had lived for some years in the West, making it even easier for them to operate in the United States.

- Once in the US, the hijackers were careful, with the exception of minor traffic violations, to avoid drawing law enforcement attention and even general notice that might identify them as extremists. They dressed in Western clothes, most shaved their beards before entering the US, and they largely avoided mosques.

- They received the money needed to finance their flight training and living expenses through ordinary wire transfers, generally in small enough amounts that they did not attract attention among the millions of financial transactions that occur in the US every day.

I mentioned the plot was tightly compartmented. For intelligence work, breaking into the compartment is key to gaining the precise details of a plot. We never achieved this success for the 9/11 plot. We now have several indications of this compartmentation.

- Bin Ladin himself—in a candid videotape found in Afghanistan after the attacks—said even some members of his inner circle were unaware of the plot.

- He also indicated that some of the hijackers themselves never knew the targets.

- Based on what we know today, the investigation of the 9/11 attacks has revealed no major slip in the conspirators' operational security.

My third characterization of the plot was to call it **resilient**. This was not a fragile plot that would have collapsed had the US government been able to achieve a few successes. In fact, the plot went forward despite several real blows.

- Flight 77 hijackers Nawaf al-Hazmi (#14) and Khalid al-Mihdhar (#12) tried to learn to fly in May 2000 and quickly had to abandon their efforts because of their poor technical and English-language skills. But by the end of 2000, a replacement pilot for Flight 77, Hani Hanjur (#11), was in

the US.

- In probably the most notable example of the plot's resilience, two members of Mohammad Atta's (#1) Hamburg cell--Ramzi Binalshibh and Zakaria Essabar--appear to have intended to join the hijackings but were denied visas multiple times. Binalshibh ended up supporting the hijacking logistically from abroad.

- Muhammad Atta (#1) himself, the pilot of the first plane to hit the World Trade Center, was stopped upon re-entering the US from Spain in January 2001 because of questions regarding his application for a change in visa status and was issued a court summons for driving without a license in April, but was not panicked by either incident.

- Most important, even after 16 August 2001 arrest of Zacarias Moussaoui--currently under indictment for conspiracy to commit terrorism and aircraft piracy, among other charges--the plan was not aborted. In fact, the hijackers began buying their tickets for 11 September just over a week after Moussaoui's arrest.

Keep these characterizations in mind as Director Mueller and I walk you through the details of the plot. Also keep in mind that the 9/11 investigation is ongoing, and we expect to know even more in the future than we present to you here today.

Let me start with <u>what we knew before the 9-11 attacks</u>:

- We knew, and warned, that Usama Bin Ladin and his al-Qa'ida organization were "the most immediate and serious" terrorist threat to the US. We said that in several ways, including in my statement to the SSCI in February 2001.

- In the months prior to 11 September, we alerted policymakers that operations that al-Qa'ida had in motion were likely to cause large-scale loss of life and be spectacular in nature.

- Beginning in June 2001, we received a barrage of intelligence indicating that al-Qa'ida associates in Afghanistan and abroad expected imminent attacks against unspecified US interests.

- Over the summer of 2001, it became evident that multiple attacks were in the works, especially abroad. Some of these were interdicted, such as planned attacks against US targets in Europe and the Middle East—successes for US intelligence.

- Finally, we knew—and warned—of Bin Ladin's desire to strike inside the US.

Malaysia

A major question surrounding the 9/11 investigation is how the United States government was able to identify two of the hijackers as al-Qa'ida but not uncover the plot they were part of. To explain how the intelligence case against Nawaf al-Hazmi (#14) and Khalid al-Mihdhar (#12) developed, I'll walk you through the case.

We had learned in late 1999 that two suspect Bin Ladin operatives, "Nawaf" and "Khaled," were planning to meet in Malaysia. At that point we only knew of their first names, and only suspected that they might be Bin Ladin operatives because of an indirect link between them and Al-Qa'ida and Egyptian Islamic Jihad operatives.

Based solely on this tenuous link, CIA initiated an operation to place "Khaled" under surveillance. Recall that we did not know either Khaled's or Nawaf's true identities at this time. The subsequent operation to learn more involved eight stations and bases and a half-dozen liaison services.

Our interest in monitoring the meeting was based on our suspicion that Khaled's travel to Malaysia was associated with supporting regional terrorist plans or operations. We believed that the meeting was likely for discussion of regrouping from extensive disruptions around the world that the CIA had engaged in.

In early 2000, just before he arrived in Malaysia, we acquired a copy of "Khaled's" passport, which showed a US multiple entry visa issued in Jeddah in April 1999 and expiring on 6 April 2000.

It is at this point that we learned that "Khaled's" name was Khalid bin Muhammad bin 'Abdallah al-Mihdhar (#12) This was the first point at which CIA had complete biographic information on al-Mihdhar.

On 5 January 2000, the US intelligence community widely disseminated an information report advising that "Khaled", identified as an individual with ties to members of the Bin Ladin organization, had arrived in Malaysia.

It was not until 5 March 2000 that we obtained information from one of our overseas stations that enabled us to identify "Nawaf" as Nawaf al-Hazmi (#14). This was the earliest time that CIA had full biographic information on al-Hazmi (#14). By that time, both al-Hazmi (#14) and al-Mihdhar (#12) had entered the US, arriving on 15 January 2000 in Los Angeles.

- The Malaysia meeting took on greater significance in December 2000 when the investigation of the October 2000 USS Cole bombing linked some of Kahlid al-Mihdhar's Malaysia connections with Cole bombing suspects. We further confirmed the suspected link between al-Mihdhar and al-Hazmi and an individual thought to be one of the chief planners of the Cole attack, via a joint FBI-CIA HUMINT asset. This was the first time that CIA could definitively place al-Hazmi and al-Mihdhar with a known al-Qa'ida operative.

- In August 2001, because CIA had become increasingly concerned about a major attack in the United States, we reviewed all of our relevant holdings. During that review, it was determined that al-Mihdhar (#12) and al-Hazmi (#14) had entered the US on 15 January 2000, that al-Mihdhar had left the US on 10 June 2000 and returned on 4 July 2001, and that there was no record of al-Hazmi leaving the country. On 23 August 2001, CIA sent a Central Intelligence Report to the Department of State, FBI, INS, and other US Government agencies requesting that al-Hazmi and al-Mihdhar be entered into VISA/VIPER, TIPOFF, and TECS [Treasury Enforcement Communication System]. The message said that CIA recommends that the two men be watchlisted immediately and denied entry into the US.

The fact that earlier we did not recommend al-Hazmi (#14) and al-Mihdhar (#12) for watchlisting is not attributable to a single point of failure. There were opportunities, both in the field and at Headquarters, to act on developing information. The fact that this did not happen--aside from questions of CTC workload, particularly around the period of the disrupted Millenium plots--pointed out that a whole new system, rather than a fix at a single point in the system, was needed.

What we know of the plot now

We have assembled a body of details that give a pretty clear picture of the plot. *Several things allowed us to assemble large amounts of information after the attacks that were not available before the attack.*

- First of all, the investigation quickly established the **hijackers' identities**. Some hijackers were identified by air crews and passengers who made phone calls from the hijacked planes, while analysis of the flight manifests, which the airlines provided immediately, revealed patterns among certain Arab nationals in first or business class: they had purchased one-way tickets and some had used the same telephone numbers or addresses when making their reservations.

- Second, some of the hijackers left behind both identifying and incriminating evidence. Muhammad Atta's (#1) luggage, for instance, had not made it onto Flight 11 from a connecting flight and contained the

guidance on preparing for an operation that was found both at the site of the Flight 93 crash in Pennsylvania and in a Flight 77 hijacker's car at Dulles Airport.

- Third, the sheer magnitude of the attacks prompted both intelligence services and journalistic organizations worldwide to put a major and immediate effort into the investigation. Friends, associates, and family members of the hijackers were interviewed by liaison services and often by reporters, which allowed us to build up a picture of the men involved.

*The operation fell into **three general stages: conceptualization, preparation,** and **execution**.*

Conceptualization

We now believe that a common thread runs between the first attack on the World Trade Center in February 1993 and the 11 September attacks. We also know that a high-ranking al-Qa'ida member was either the mastermind or one of the key planners of the 11 September operation.

- Mukhtar is the uncle of Ramzi Yousef, who masterminded the 1993 bombing plot against the World Trade Center.

- Following the 1993 attack, Yousef and Mukhtar plotted in 1995 to blow up US planes flying East Asian routes--for which Mukhtar was indicted in 1996. Philippine authorities uncovered the plot in January 1995 and Yousef was apprehended the following month, but Mukhtar escaped.

- Yousef also considered flying a plane into CIA headquarters, according to one of his co-conspirators [Murad], who was interrogated by Philippine authorities in 1995.

Mukhtar was not the only Bin Ladin associate to consider how to use commercial airliners in terrorist attacks.

- After 11 September, we learned that in 1996, Bin Ladin's second-in-command, Muhammad Atif, drew up a study on the feasibility of hijacking US planes and destroying them in flight, possibly influenced by Yousef's and Mukhtar's unrealized plans.

Bin Ladin's determination to strike America at home increased with the issuance of the February 1998 fatwa targeting all Americans, both military and civilian. The ideas about destroying commercial airliners that had been circulating in al-Qa'ida leadership circles for several years appear to have been revived after that

fatwa.

- Although we lack details on exactly when the plan was formulated and received Bin Ladin's approval, we know that the planning for the attacks began three years before 11 September.

- We understand that when one of his associates proposed to Bin Ladin that the World Trade Center be targeted by small aircraft packed with explosives, Bin Ladin reportedly suggested using even larger planes.

- We also believe that outside events also shaped al-Qa'ida leaders' thinking about an airliner attack. The October 1999 crash of Egypt Air Flight 990, attributed in the media to a suicidal pilot, may have encouraged al-Qa'ida's growing impression that air travel was a vulnerability for the US.

In December 1999, the plot moved from conceptualization to preparation, with the arrival in Afghanistan of three young Arab men from Hamburg, Germany who would become pilot-hijackers on 11 September.

Preparation

The men selected to carry out the 11 September attacks largely fall into three overall categories:

- The three pilots from Hamburg I just mentioned;

- Al-Qa'ida veterans;

- And young Saudis.

The Hamburg Cell

The men from Hamburg were Muhammad Atta (#1), Marwan al-Shehhi (#6), and Ziad Jarrah (#16), on whom the US held no derogatory information prior to 11 September 2001.

- They were part of a group of young Muslim men in Hamburg, Germany who came from different countries and backgrounds, but attended the same mosques, shared common acquaintances, and were drawn together by their increasingly extreme Islamist views and disenchantment with the West.

- **They were *intelligent, English-speaking, and familiar with Western society—traits crucial to carrying out the 11 September plot.***

- ***They were well suited--educated, including in technical subjects, and proficient in several languages--to mastering the skills they would need to pilot three of the four planes on September 11.***

Muhammad Atta (#1), an educated middle-class Egyptian, arrived in Hamburg in 1992.

- Atta did not exhibit any signs of extremism before leaving for Germany, but Atta was open with his German acquaintances about his dissatisfaction with Egypt's increasing Westernization, what he perceived as the Egyptian government's corruption and persecution of the Muslim Brotherhood, and his antipathy toward Israel.

- Atta became increasingly devout during his time in Germany and friends have also reported that Atta became increasingly pessimistic about his prospects for employment and expression of his religious and political beliefs back in Egypt. By 1997, Atta appears to have lost contact with most of his German friends and was associating almost exclusively with other Muslims.

- Atta may have traveled to Afghanistan for the first time in early 1998 when he told his roommate he was gone for two months on a pilgrimage. During a trip to Egypt in June, Atta applied for a new passport, even though his old one had not yet expired, suggesting that he might have been trying to hide evidence of travel to Afghanistan. (

Future hijacker-pilot **Marwan al-Shehhi (#6)**, came to Germany from the United Arab Emirates in April 1996 on a UAE military scholarship.

- We believe he lived in *Bonn* through early 1999, when he passed a German proficiency exam, but apparently was a visitor to *Hamburg* before 1999.

- Marwan Al-Shehhi moved to Hamburg in 1999 and enrolled at the Hamburg-Harburg Technical University where Atta studied.

Ziad Jarrah (#16), like Atta, came from a middle-class family.

- Having dreamed of becoming a pilot since childhood, Jarrah traveled from his home in Lebanon to Germany to study in 1996.

- At some point during the time he spent in Greifswald from 1996 to 1997, Jarrah appears to have come in contact with Abdulrahman al-Makhadi, an imam at a Greifswald mosque suspected of having terrorist connections.

- Jarrah moved to Hamburg in August 1997 where he began studies in aircraft construction at Hamburg's School of Applied Sciences.

- Fellow students have told the press that while he was devout and prayed five times a day, he never struck them as an extremist. (S//NF)

A common acquaintance of members of Atta's circle was German-Syrian Muhammad Heydar Zammar, a known al-Qa'ida associate in Hamburg who was detained after 11 September.

- Zammar has been active in Islamic extremist circles since the 1980s and first trained and fought in Afghanistan in 1991 He trained and fought in Bosnia in and made many return trips to Afghanistan.

- Zammar met Atta (#1), al-Shehhi (#6), and Jarrah (#16) (along with others of the Hamburg cell) in the late 1990s at the Hamburg al-Qods mosque and persuaded them to travel to Afghanistan to join the jihad.

Atta's (#1) relationship with his roommate, Yemeni Ramzi Binalshibh, may also have been crucial in focusing the Islamist beliefs of the Hamburg circle on al-Qa'ida. Since 11 September, we have received a variety of reports identifying Binalshibh as an important al-Qa'ida operative and we suspect that, unlike the three Hamburg pilots, he may have been associated with al-Qa'ida even before moving to Germany in 1995.

The al-Qa'ida Veterans

We now know that two of the hijackers had been involved with al-Qa'ida for several years before 11 September 2001.

- They were Saudis Nawaf al-Hazmi (#14) and Khalid al-Mihdhar (#12), who on 11 September would help to hijack American Airlines Flight 77 that crashed into the Pentagon. We have learned a great deal about these men since 11 September

- The two men grew up together in Mecca.

- In the mid-90s, al-Hazmi (#14) and al-Mihdhar (#12) traveled to Bosnia.

- Afterward their involvement with Al-Qa'ida strengthened. Al-Hazmi traveled to Afghanistan sometime before 1998 and swore loyalty to Bin Ladin. Later, Al-Mihdhar (#12) also traveled to Afghanistan and swore his allegiance to Bin Ladin.

- Al-Hazmi (#14) and al-Mihdhar (#12) returned to Saudi Arabia in early 1999. In April, both men obtained visas from the US consulate in Jeddah.

The Young Saudis

The young Saudi men who made up the bulk of the support hijackers became involved with al-Qa'ida in the late 1990s, we have learned since 11 September.

- Many, like veterans al-Hazmi (#14) and al-Mihdhar (#12), knew each other before they traveled to Afghanistan and became involved in the 11 September operation.

- Investigative efforts have uncovered two sets of brothers--the al-Hazmis (#14 and #15) and al-Shehris (#4 and #5)—as well as small networks of friends and acquaintances among the young Saudi hijackers, many of whom came from southwest Saudi Arabia.

- They came from a variety of backgrounds--their families came from different parts of the socioeconomic spectrum, and a few had higher education while others had little at all. Some had struggled with depression or alcohol abuse, or simply seemed to be drifting in search of purpose.

- Some of these young men had reportedly never exhibited much religious fervor, before apparent exposure to extremist ideas--through family members, friends, or clerics--led to an abrupt radicalization and separation from their families.

As part of their commitment to militant Islam, these young Saudis traveled to Afghanistan to train in the camps of their exiled countryman Usama Bin Ladin.

- An analysis of travel data acquired since 11 September suggests that most went to Afghanistan for the first time in 1999 or 2000, traveling through one or more other countries before entering Afghanistan to disguise their destination.

- Only for Fayez Banihammad (#8) of the United Arab Emirates has no information emerged suggesting travel to Afghanistan, although it is reasonable to assume that he was there at some point before entering the US.

- Although their early travel to Afghanistan added these young men to the ranks of operatives that al-Qa'ida could call upon to carry out future missions, we do not believe that they became involved in the 11 September plot until late 2000 [we don't believe the al-Qa'ida leadership

would have wanted them knowing about a plot in the US any sooner than necessary given the conspiracy's compartmentation]. Even then, they probably were told little more than that they were headed for a suicide mission inside the United States.

Saudi **Hani Hanjur** (#11), the fourth pilot, is similar to the other young Saudi hijackers in some ways, yet stands out because of:

- His prolonged and frequent presence in the US prior to 11 September.
- His lack of known ties to other Saudi hijackers prior to becoming involved in the conspiracy.
- His probable role as a pilot on 11 September, given that he had far greater flying experience than Flight 77 co-hijackers Nawaf al-Hazmi and Khalid al-Mihdhar.

Hani Hanjur (#11) expressed an early wish to participate in a jihad conflict, but did not appear to experience a sudden increase in his religious fervor until 1992. That year, he returned to Saudi Arabia after four-and-a-half months in the US "a different man," according to one of his brothers who spoke to the Western media. Hanjur reportedly now wore a full beard, cut his past social ties, and spent most of his time reading books on religion and airplanes. In April 1996, Hanjur returned to the US.

The Hamburg pilots traveled to Afghanistan in late 1999 at which time they were likely selected for and briefed on the 11 September plot.

- Atta (#1) flew from Hamburg to Istanbul in late 1999, then on to Karachi, Pakistan. After that, he evidently traveled into Afghanistan.
- According to information acquired after the 11 September attacks, Atta (#1) and al-Shehhi (#6) were both present at Bin Ladin facilities in Afghanistan in late 1999; Atta's presence has been corroborated by a separate source.
- Al-Shehhi (#6) likely left Hamburg at roughly the same time as Atta (#1) since he granted power of attorney over his German bank account to another member of the Hamburg cell beginning November 1999.
- Jarrah's (#16) travel at this time mirrored Atta's, flying from Hamburg to Istanbul and then on to Karachi in late 1999.

Since 11 September we have also obtained information on **which al-Qa'ida leaders were involved** in planning the attacks during this crucial late-1999

period in Afghanistan.

- We know that Bin Ladin deputy Muhammad Atif deliberately chose the hijackers from young Arab men who had no previous terrorist activities.

- The hijackers were also chosen on the basis of nationality so that they would not have trouble obtaining US visas. Another senior Bin Ladin lieutenant then arranged for them to get pilot training.

- *Khallad (AKA Walid Ba 'Attash)*, a key planner of the 2000 attack on the *USS Cole*, was also in Afghanistan at this time.

- We also believe that an Al-Qa'ida military committee consisting of key Al-Qa'ida operatives was supportive and aware of the operation and its stages..

When they left Afghanistan at the end of 1999 and early 2000, the Hamburg hijackers immediately began to prepare for their mission.

- They began by acquiring new passports that would show no sign of travel to Afghanistan when they applied for US visas.

- Al-Shehhi (#6) obtained a new passport and a US visa in the UAE in January 2000.

- Jarrah (#16) returned to Hamburg in January and on 9 February 2000, reported that his passport had been lost. He received a visa from the US Embassy in Berlin in May 2000.

- Atta (#1) returned to Hamburg in February 2000. In March, he sent e-mails to flight schools in Florida and Oklahoma asking about pilot training. Atta received a new Egyptian passport from the Egyptian consulate in Hamburg on 8 May 2000. On the 18th, he was issued a visa by the US Embassy in Berlin.

Al-Shehhi (#6), Atta (#1), and Jarrah (#16) entered the US on different dates in May and June 2000, from three different European cities, possibly to mislead authorities as to their common purpose.

- Al-Shehhi (#6) flew from Brussels to Newark on 29 May 2000.

- Atta (#1) traveled by bus to Prague, entering the city on 2 June 2000, and flew to Newark the next day.

- Jarrah (#16) flew from Dusseldorf to Newark, and then on to Venice, Florida, on 27 June 2000.

While the Hamburg pilots were wrapping up their training in Afghanistan and returning to Germany in late 1999 and early 2000, halfway around the world the al-Qa'ida veterans, Nawaf al-Hazmi (#14) and Khalid al-Mihdhar (#12), prepared to enter the US.

- After receiving US visas in April 1999, both men had traveled to Afghanistan and participated in special training in the latter half of 1999. This training may have been facilitated by Khallad.

- After the January 2000 Malaysia meeting outlined earlier, they entered the US on 15 January.

As you may have already noticed, the inclusion of al-Hazmi (#14) and al-Mihdhar (#12) in the plot seems to violate one of the conspiracy's most successful tactics: the use of untainted operatives. Unlike the other hijackers, al-Hazmi (#14) and al-Mihdhar (#12) had years of involvement with al-Qa'ida--to such an extent that they had already come to our attention before 11 September. Without the inclusion of al-Hazmi (#14) and al-Mihdhar (#12) in the plot, we would have had none of the hijackers who died on 11 September in our sights prior to the attacks. We speculate that this difference may be explained by the possibility that the two men originally entered the US to carry out a different terrorist operation prior to being folded into the 9/11 plot. I'll briefly outline the factors, other than their long track record with al-Qa'ida, that have led us to consider this possibility.

- Al-Hazmi (#14) and al-Mihdhar (#12) **obtained US visas far earlier** than the other hijackers--in April 1999, while the Hamburg pilots didn't begin getting US visas until early 2000.

- As noted above, al-Hazmi (#14) and al-Mihdhar (#12) received **special training in Afghanistan** in the latter half of 1999, along with *USS Cole* suicide bomber al-Nibras and a key planner of the *Cole* attack, Khallad. None of the other hijackers are known to have received this training and the Hamburg pilots visited Afghanistan after al-Hazmi and al-Mihdhar had apparently departed.

- Al-Hazmi (#14) and al-Mihdhar (#12) **interacted far more with the local Arab population** when they settled in the US than did the other hijackers.

- Pilots Atta (#1), al-Shehhi (#6), Jarrah (#16), and later Hanjur (#11) all began flight training quite soon after arriving in the US, while al-Hazmi (#14) and al-Mihdhar (#12) **did not engage in flight training activity until April 2000**--approximately three months after coming to this country. (S//HCS,NF)

As mentioned earlier, it appears that at least one other member of the Hamburg cell--and possibly two--intended to participate in the 11 September attacks as a pilot.

- Yemeni Ramzi Binalshibh, a close associate and roommate of Atta (#1) in Germany, failed on multiple occasions in 2000 to obtain a US visa and even sent a deposit to the flight school where Jarrah (#16) was training.

- After Binalshibh's efforts failed, another cell member, Moroccan Zakaria Essabar, tried and failed to obtain a visa in January 2001; he was also trying to travel to Florida.

- Both men displayed the same tradecraft that characterized the other hijackers: persistence in the face of obstacles, an evident decision to enter the country legally and under true name, and flexibility regarding their roles in the plot. Binalshibh, for instance, transferred money to Marwan al-Shehhi (#6) in 2000 while still attempting to acquire a US visa.

The entry of the future pilots into the US also launched the financing of the plot in earnest. The financial transactions that supported the attacks in many ways reflected the overall nature of the operation, relying on ostensibly legitimate activities carried out inside the US over the course of nearly two years. Key characteristics of the financial support operation included:

- **Long-term planning.** Transfers of significant funds related to the operation began nearly two years before the attacks and appear to have been calculated to cover specific training and travel needs.

- **Division of labor.** Each hijacker appears to have been responsible for maintaining his own account and personal transactions, while three hijackers--Atta (#1), al-Shehhi (#6), and Banihammad (#8)--generally assumed responsibility for communicating with financial facilitators, receiving and returning funds, and distributing money to other hijackers.

- **Pervasive use of cash.** The plotters used cash to open accounts and effectively concealed their day-to-day activities through cash withdrawals rather than check or credit transactions.

- **Trickle-down through intermediaries.** The plotters obscured the operation's ultimate funding sources by sending funds through various individuals before reaching the final recipient.

- **Exploitation of open economies.** The operation's principal financial hubs were the UAE, Germany, and the US, partly because of the relative

ease and anonymity with which financial transactions can be conducted in these countries.

- **External funding**. Virtually all of the financial support for the attacks came from abroad.

As training for the pilot-hijackers proceeded in the US through the latter half of 2000, al-Qa'ida leaders turned their attention to bringing into the plot the young men who would support the pilots.

- Most of the young Saudis obtained their US visas in the fall of 2000. The State Department did not have a policy to stringently examine Saudis seeking visas prior to 11 September because there was virtually no risk that Saudis would attempt to reside or work illegally in the US after their visas expired. US Embassy and consular officials do cursory searches on Saudis who apply for visas, but if they do not appear on criminal or terrorist watchlists they are granted a visa. Thousands of Saudis every year are granted visas as a routine--the majority are not even interviewed. The vast majority of Saudis study, vacation, or do business in the US and return to the kingdom.

- Reporting suggests that all of them--possibly including pilot Hani Hanjur (#11)--then traveled to Afghanistan at some point in late 2000 or early 2001.

On 3 January 2001, **Atta** (#1) flew from Tampa, Florida to Madrid, Spain. No details have yet emerged on the week he spent in Spain, although it may have been to meet with another al-Qa'ida operative to pass along an update on the pilots' training progress and receive information on the supporting hijackers who would begin arriving in the US in the spring. On 10 January, Atta returned to the US, flying from Madrid to Miami.

Atta (#1) was not the only pilot to travel outside the US during the period when he was attaining and honing his flying skills.

- **Jarrah** (#16) left the US six times, apparently spending most of his time outside the US visiting either family in Lebanon or his girlfriend in Germany.

- **Al-Shehhi** (#6) also traveled outside the US, flying to the UAE, Germany, Morocco, and Egypt on three different trips. While it is known that al-Shehhi visited Atta's (#1) father during his April 2001 trip to Egypt to collect Atta's international driver's license, nothing else is known of al-Shehhi's activities while traveling outside the US.

As you may have read in the press, **Atta** (#1) allegedly traveled outside the US in early April 2001 to meet with an Iraqi intelligence officer in Prague, we are still working to confirm or deny this allegation.

- It is possible that Atta (#1) traveled under an unknown alias since we have been unable to establish that Atta left the US or entered Europe in April 2001 under his true name or any known aliases.

Khalid al-Mihdhar (#12) returned to the US on 4 July 2001 after nearly a year out of the country. He had spent the past year traveling between Yemen and Afghanistan, with occasional trips to Saudi Arabia.

- Al-Mihdhar (#12) returned to Saudi Arabia in June and on 13 June obtained a US visa in Jeddah

In July 2001, **Atta** (#1) **returned to Spain.** On 7 July, he flew from Miami to Zurich, then on to Madrid.

- After checking out of a Madrid hotel on the 9th, Atta's (#1) movements are unknown for several days.

- His next known location is in Tarragona on Spain's east coast on 13 July, when he checked into a local hotel.

- After moving on to two other hotels, Atta (#1) returned to Madrid and flew back to Florida on 19 July.

- Although nothing specific is known of Atta's (#1) activities while in Spain, fellow conspirator Ramzi Binalshibh from Hamburg flew from Germany to Tarragona on 9 July 2001. He checked out of a local hotel the next day and his whereabouts from 10 to 16 July are unaccounted for, roughly the same period during which Atta's movements are unknown, suggesting the two engaged in clandestine meetings on the progress of the plot.

- We are continuing to investigate Atta's (#1) and Binalshibh's activities and possible contacts while in Spain.

Conclusion

By 5 August 2001, all of the hijackers are in the United States to stay. Before I turn to Director Mueller to describe what the plotters did in the United States, let me conclude with a few points:

The lessons of 11 September have not just been learned, but acted on.

- In this struggle, we must play offense as well as defense. The move into the Afghanistan sanctuary was essential. We have disrupted the terrorists plans, denied them the comfort of their bases and training facilities and the confidence that they can mount and remount attacks without fear of serious retribution.

- The drive into the sanctuary has led to the uncovering of and at least partially foiling Bin Ladin's plans to develop weapons of mass destruction. The capture of many high ranking and low-level al-Qa'ida members has disrupted the al Qa'ida infrastructure and has given us leads to other cells and networks.

- I have said we have been working closely with the FBI, and our cooperation has grown even closer since 9/11. Director Mueller and I are working to deepen that cooperation. Specifically, CIA is helping to build an FBI analytic capability. We are also working to extend the good cooperation we have built between our chiefs of station and legal attaches overseas to a system of cooperation between CIA and FBI field offices in the United States.

- We have significantly increased the number of CIA officers analyzing terrorist patterns and trends. More needs to be done to give our Counterterrorist Center the people, both in numbers, experience, and continuity, to make certain that every lead is followed to the utmost of our capability.

- And our support to watchlisting is being revamped. Standardized guidance has been distributed to CTC officers on watchlist procedures, reminding them to err on the side of reporting when sending names to the Department of State. In addition, language has been established that can be inserted into intelligence reports that flags information to review by the State Department for inclusion in the Visa Viper system. Beyond CIA, a National Watch List Center is being designed that would be accessible to all relevant federal agencies; a database has been created so that State, FBI, DoD, FAA, INS, Customs, and Treasury representatives who sit in CTC can easily access it; and CTC is creating a unit within the center that will be dedicated to reviewing names and ID-related data fragments for watchlisting.

- As important as understanding and learning from the 9/11 plot is, we need to meet in a subsequent session so you can objectively assess the full scope of our counterterrorist effort from the early 1990's through the present.

Ongoing security enhancements and the development of new leads, investigations and human sources, have made it harder for identical attacks to take place. However, al-Qa'ida is known for changing its tactics, and a determined group of terrorists, using a slightly different approach, could succeed if they used much of the resilient tradecraft employed by the 11 September hijackers.

- Al-Qa'ida's tradecraft, combined with the enormous volume of travelers entering the US every year, will make it impossible to guarantee that no terrorists will enter the country.

- The type of financial transactions and communications used by the hijackers would still be lost among the millions of others taking place in the US every day without preexisting information to draw attention to the initiators.

- Based on what what we have learned about the 11 September plot, an attempt to conduct another attack on US soil is certain.

- Even with the increased government and public vigilance employed against terrorism since 11 September, the danger is still great.

Chairman GRAHAM. Ms. Hill, please proceed.

Ms. HILL. Thank you, Mr. Chairman. I have one additional administrative item before beginning my statement.

That is, the Members may recall that on September 24 we held an open hearing at which I presented a staff statement regarding the FBI's handling of the Phoenix electronic communication and the investigation of Zacarias Moussaoui prior to September 11. At the time of that hearing, we presented a statement that had been in part redacted due to concerns about the ongoing criminal case with Mr. Moussaoui. At that hearing or right before that hearing we received an order from the judge in that case which then allowed us to pursue what the Justice Department and the FBI—expanding or eliminating some of the redactions that we had made in the initial statement.

Last night we received back from the CIA, and also having gone through the Justice Department and the FBI, a revised version, expanded version of what we presented at the September 24 hearing. I'd like to offer this as part of the record, in that it has added more information from the original classified version that has now been cleared for public release.

Chairman GRAHAM. Is there objection?

Without objection, so ordered.

[The information referred to follows:]

The FBI's Handling of the Phoenix Electronic Communication and Investigation of Zacarias Moussaoui Prior to September 11, 2001
Eleanor Hill, Staff Director, Joint Inquiry Staff
September 24, 2002
[As Supplemented October 17, 2002]

Introduction

Mr. Chairmen, members of this Joint Committee, good morning. I appreciate the opportunity to appear before the Committees once again. At our last hearing, we discussed information the Intelligence Community had available prior to September 11, 2001 regarding the September 11 hijackers. Today, I will discuss:

- The July 10, 2001 electronic communication (EC) from the FBI's Phoenix field office to FBI headquarters," also known as the "Phoenix memo"; and

- The investigation, prior to September 11, 2001, of Zacarias Moussaoui.

As I mentioned in discussing our work concerning the September 11 hijackers, I want to again emphasize the significance of these areas when viewed collectively. Three areas were available in the same section at the Federal Bureau of Investigation's (FBI) headquarters in late August 2001. Two of these areas were addressed in the Director of Central Intelligence's (DCI) Counterterrorist Center (CTC) at approximately the same time. No one apparently saw the potential collective significance of this information, despite the increasing concerns throughout the summer of 2001 of an impending terrorist attack.

The Phoenix Electronic Communication

The Joint Inquiry Staff's interim statement to the Committees on September 18, 2002 discussed the indications of an impending terrorist detected by the Intelligence Community in the summer of 2001 and the warnings that intelligence resulted in. In that same timeframe, an FBI special agent in the FBI's Phoenix field officer generated a document that has been subsequently described in media reports as the "Phoenix memo." It is known within the FBI as the Phoenix Electronic Communication, or "Phoenix EC." "EC" is an FBI term of art. ECs are the primary type of document used by the FBI for internal communications. In this statement, we use the terms "Phoenix memo" and "Phoenix EC" interchangeably.

The Joint Inquiry Staff reviewed the Phoenix EC and its handling by FBI headquarters with the following questions in mind:

- What did the EC say?
- Why did the special agent write it?

- Who handled it within FBI headquarters and what reaction did it elicit?
- Does FBI headquarters' handling of the document illuminate any broader, systemic problems within the FBI?

Introduction

On July 10, 2001, a Special Agent (SA) in the FBI's Phoenix Division sent an EC to individuals in the Usama Bin Ladin Unit (UBLU) and the Radical Fundamentalist Unit (RFU) within the Counterterrorism Division at FBI headquarters and to several SAs on an International Terrorism squad in the New York Field Office. In the EC, the SA outlined his concerns that there was a coordinated effort underway by Usama Bin Ladin to send students to the United States for civil aviation-related training. He noted that there were an "inordinate number of individuals of investigative interest" attending this type of training in Arizona and speculated that this was part of an effort to establish a cadre of individuals in civil aviation, who would be in position to conduct terrorist activity in the future.

The EC contained a number of recommendations that the agent asked FBI headquarters to consider implementing. Apparently, the communication did not raise any alarms at FBI headquarters or in the New York office. In fact, New York personnel who reviewed the EC found it to be speculative and not particularly significant. New York already knew that many Middle Eastern flight students, including several associated with Bin Ladin, trained in the United States. They believed that Bin Ladin needed pilots to transport goods and personnel in Afghanistan, and, at the time, viewed pilots connected to Bin Ladin in that light. About a week after its receipt, headquarters personnel determined that no follow-up action was warranted on the Phoenix EC recommendations. No managers at FBI headquarters took part in that decision or even saw the communication before September 11, 2001. No one apparently considered the significance of the Phoenix EC in light of what else confronted the FBI counterterrorist team during the summer of 2001: the unprecedented increase in terrorist threat reporting, the investigation and arrest of Zacarias Moussaoui in August 2001, and the possible presence of Bin Ladin associates al-Mihdhar and al-Hazmi in the United States.

Our review of the circumstances surrounding the Phoenix memo reveals a number of weaknesses at the FBI that, if left uncorrected, will continue to undercut counterterrorist efforts. The FBI handling of the Phoenix EC is symptomatic of a focus on short-term operational priorities, often at the expense of long-term, strategic analysis. Throughout this review, we have found that the FBI's ability to handle strategic analytic products, such as the Phoenix EC, was, at best, limited prior to September 11, 2001. Inadequate information sharing within the FBI, particularly between the operational and analytic units, is also highlighted by our review of the Phoenix EC. Several of the addressees on the EC, especially at the supervisory level, did not receive it prior to September 11 due to limitations in the electronic dissemination system. Those limitations are consistent with the complaints we have repeatedly heard throughout this inquiry about the FBI's technology problems. Finally, the case-driven, law enforcement approach, while important and extremely productive in terms of the FBI's traditional mission, does

not generally "incentivize" attention to big-picture, preventive analysis and strategy. This is particularly true where there is no direct and immediate impact on an ongoing criminal prosecution.

In that context, the Joint Inquiry Staff found that the Phoenix memo was not the first time the FBI had confronted concerns about Middle Eastern individuals studying aviation topics in the United States. In 1998, the FBI's chief pilot in Oklahoma City drafted a memo expressing concern about the number of Middle Eastern flight students there and his belief that they could be planning a terrorist attack. Also in 1998, the FBI had received reporting that a terrorist organization planned to bring students to the United States to study aviation and that a member of that organization had frequently expressed an intention to target civil aviation in the United States. Yet another terrorist organization, in 1999, allegedly wanted to do the same thing, triggering a request from FBI headquarters to 24 field offices to investigate and determine the level of the threat. To date, our review has found that the field offices conducted little to no investigation in response to that request.

Our inquiry found that, given the lack of information sharing across units in FBI headquarters, personnel who saw the Phoenix memo had no knowledge of any of these prior instances involving other terrorist groups. Since the prior reporting did not directly relate to al-Qa'ida, they were unable to evaluate the Phoenix EC in the context of what was known about likely terrorist strategies favored by other, similar groups. As terrorist groups increasingly associate with and support each other, information sharing and overarching strategic analysis is critical to success in counterterrorist efforts. This is particularly important to the FBI's efforts here in the United States, where the members of the various groups tend to associate with each other.

Finally, while the Phoenix EC does not include by name any of the hijackers involved in the September 11, 2001 attacks, our review confirmed that the FBI now believes that one of the individuals named in the EC was connected to Hani Hanjour, who is now believed to have piloted American Flight 77. The individual named in the EC has been connected both through witness statements and flight school records to Hanjour. This individual first came to the attention of the FBI in 1999, but when the FBI went to investigate him, they determined that he had left the United States, and an investigation was not opened. The FBI was apparently unaware that he had returned to the United States in the summer of 2001 and may have been associating with Hanjour and several other Islamic extremists. These issues will be discussed at greater length in subsequent sections.

Summary of the Phoenix EC

In an interview with the Joint Inquiry Staff, the special agent in Phoenix who wrote the EC said that he first became concerned about aviation-related terrorism in the early 1990s. He was working on two cases in which Libyans with suspected terrorist ties were working for U.S. aviation companies. One of these individuals had a Masters degree in a technical field, yet was working in menial jobs at the airport as a skycap and

then a baggage handler. The other individual was working as a technical avionics officer for a domestic airline and was charged with overseeing the complete overhaul of aircraft and with checking for structural integrity. In addition, several Bin Ladin operatives had lived and traveled to the Phoenix area in the past, one of whom was Wadih El-Hage, a Bin Ladin lieutenant convicted for his role in the 1998 embassy bombings. He had lived in the Tucson area for several years in the 1980s. The Phoenix SA believes that El-Hage established a Usama Bin Ladin support network in Arizona while he was living there and that this network is still in place.

The agent stated that the idea of possible terrorists having easy access to aircraft conjured up visions of Pan Am 103. The Phoenix agent told the Joint Inquiry Staff that, in authoring the EC, he never imagined terrorists using airplanes as was done on September 11. His primary concern was that Islamic extremists, studying everything from aviation security to flying, could be learning how to hijack or destroy aircraft and to evade airport security.

In April 2000, the agent interviewed the individual who was the subject of the Phoenix EC. When he interviews young foreign nationals they usually tend to be at least somewhat intimidated in their first contact with the FBI. By contrast, this individual told the agent directly that he considered the U.S. government and military legitimate targets of Islam. In looking around the individual's apartment, the agent noticed a poster of Bin Ladin and another poster of wounded Chechnyan mujaheddin fighters. He was also concerned by the fact that this individual was from a poor Middle Eastern country and had been studying a non-aviation related subject prior to his arrival in the United States.

The agent also described for us another incident that increased his suspicion about Middle Eastern flight students in the Phoenix area. During a physical surveillance of the subject of the Phoenix EC, the agent determined that he was using a vehicle registered to another individual. In 1999, the owner of the car and an associate of his were detained for trying to gain access to the cockpit of a commercial airliner on a domestic flight. They told the FBI that they thought the cockpit was the bathroom and they accused the FBI of racism. They were released after an investigation, the FBI closed the case, and the two were not prosecuted. A year later, the individual's name was added to the State Department's watchlist after intelligence information was received indicating that he may have gotten explosive and car bomb training in Afghanistan. In August 2001, the same individual applied for a visa to re-enter the United States and, as a result of the watchlisting, was denied entry.

In May 2001, after a brief time investigating a series of arsons, the Phoenix special agent was reassigned to work international terrorism matters. To get back up to speed, he reviewed case files of terrorism cases on his squad. In the course of the review, he became increasingly concerned by the number of individuals of potential investigative interest enrolled in aviation training. At that point, he began to draft the EC, which he completed by July 10, 2001.

The Phoenix EC focuses on 10 individuals who were the subjects of FBI investigations. These individuals were Sunni Muslim, and were from Kenya, Pakistan, Algeria, the United Arab Emirates, India, and Saudi Arabia. Not all were in flight training; several were aeronautical engineering students, and one was studying international aviation security. One of the individuals under investigation was the primary focus of the Phoenix EC.

This individual had come to the Phoenix agent's attention when it was learned that he was a member of the al-Muhajiroun, whose spiritual leader was a strong supporter of Bin Ladin and who had issued a number of *fatwas* against the United States, one mentioning airports as a possible target. The subject of the Phoenix investigation was enrolled at Embry Riddle University and was taking aviation-related security courses. As a member of the al-Muhajiroun, he was organizing anti-U.S. and anti-Israeli rallies and calling for jihad. The investigation of this individual led to the opening of investigations on six of his associates, also involved in aviation training. The remaining three subjects in the Phoenix EC, although involved in aviation subjects, were not known to associate with the others.

We asked the Phoenix agent whether he had received any intelligence from FBI headquarters or from other Intelligence Community agencies that contributed to the suspicions he raised in the EC. According to him, the Phoenix office did not receive FBI, Intelligence Community, or foreign intelligence service products on a regular basis. He told us that he believes that prior to September 11, 2001 the FBI was not running counterterrorism as a national level program; he often has felt that he's "out on an island" in Phoenix. He said that, prior to headquarters downsizing, the FBI used to do a better job of disseminating intelligence products to the field. He does not believe that sufficient resources are devoted to counterterrorism even though it is officially a Tier I program. In his words, counterterrorism and counterintelligence have always been considered the "bastard stepchild" of the FBI because these programs do not generate the statistics that other programs do, such as Violent Crimes/Major Offenders or drugs.

The Phoenix EC makes four recommendations and requests that FBI headquarters consider implementing them:

- Headquarters should accumulate a list of civil aviation university/colleges around the country;
- FBI offices should establish liaison with the schools;
- Headquarters should discuss the Phoenix theories with the intelligence community;
- Headquarters should consider seeking authority to obtain visa information on individuals seeking to attend flight schools.

Phoenix Office's Actions Prior to Sending the EC

While he was developing the EC, the Phoenix agent attended a meeting in May/June 2000 of a local intelligence working group. At the meeting the agent told the

attendees about the individual under investigation who was attending Embry Riddle University. He asked if anyone had information on Islamic extremists showing up at aviation schools. No one offered any information. The agent told the Joint Inquiry Staff that he had also discussed his theories with other members of the Phoenix Joint Terrorism Task Force. The Joint Inquiry Staff's examination of records has determined that he also requested that routine intelligence community checks be run on the subjects of the EC. In March 2001, the agent's supervisor in Phoenix attended a meeting in Long Beach where he mentioned the Phoenix theories about civil aviation. CIA was made aware of the FBI information, but had no relevant information to offer.

As he was drafting the EC, the Phoenix agent contacted an Intelligence Operations Specialist (IOS) at FBI headquarters whom he had known for a number of years to use as a sounding board. The IOS provided him with several names to include on the addressee list. Around the same time, another agent on the same Phoenix squad called the FAA's counterterrorism representative at FBI headquarters to inquire about the legality of the Middle Eastern students attending aviation schools. The FAA representative said that, as long as the students were in legal immigration status, their attendance was legal.

Headquarters' Response to the EC

When he sent the EC to the Counterterrorism Division at FBI headquarters the Phoenix agent requested in a "lead""[1] that both the RFU and UBLU consider implementing the suggested actions that he had set out. On July 30, 2001, an Intelligence Assistant (IA) in the RFU at FBI headquarters assigned the lead to an IOS. The IOS appears to have been picked, not because the assignment was within her programmatic area of responsibility, but because her name was the first non-supervisory name on the addressee list. At the time, this was typical of the way in which leads were assigned in the unit. The IOS recalls the lead arriving in her electronic folder on the system but did not receive a hard copy of the document from the IA. After reviewing the EC, the IOS determined that the project should be handled by someone in the UBLU.

The RFU IOS contacted a UBLU IOS to effect a transfer. The UBLU IOS did not want the lead transferred but agreed to take responsibility for her unit's response. The UBLU IOS also received a hard copy of the document. The UBLU IOS then consulted two other IOSs in her unit, mentioning specifically the paragraph in the EC about obtaining visa information. Their discussion centered on the legality of the proposal and whether it raised profiling issues. The IOS also decided to forward the EC to the Portland office because an individual named in the EC, with ties to suspected terrorists

[1]This is an FBI system through which the office sending a communication can request that the receiving office(s) take some follow-up action or conduct additional investigation. In the "lead" section of the communication, the sending office can outline exactly what action or investigation that it is requesting that the receiving office conduct. Once the lead has been completed (or "covered" in FBI vernacular), the receiving office will inform the sending office as to the results of the investigation or as to the action taken.

arrested in the Middle East in early 2001, was an employee of an airline and had previously lived and studied in the northwestern United States.

On August 7, 2001, after receiving no objection from the Phoenix office, the EC was forwarded to an intelligence analyst in Portland via email, stating that the document "basically puts forth a theory on individuals being directed to come here to study aviation and their ties to extremists. Nothing concrete or whatever, but some very interesting coincidences. I thought it would be interesting to you considering some of the stuff you were coming up with in PD [Portland]. Let me know if anything strikes you." The Portland analyst has told the Joint Inquiry Staff that she had spoken to the UBLU IOS on several occasions about the aviation-related ties of terrorist subjects in the Portland and Seattle areas. She did not take action on the communication or disseminate it any further, as it was only sent to her for informational purposes.

The UBLU IOS informed the Joint Inquiry Staff that she affixed a note to her copy of the EC, on which she jotted down several items to follow up on. She recalls that her first item was to review the intelligence investigations of another individual who was the only Usama Bin Ladin pilot she knew about.[2] She assumes she would have also written that she should call agents in two FBI field offices who were familiar with this individual. The note was on her copy of the EC that she provided to the Department of Justice Inspector General (IG). The IG has informed the Joint Inquiry Staff that they recall seeing the note during their interview of the IOS but cannot locate it.

On August 7, 2001, both IOSs decided that the lead should be closed. In the electronic system, the RFU IOS noted that the lead was "covered- consulted with UBLU, no action at this time, will reconvine [sic] on this issue." The UBLU IOS maintains that she fully intended to return to the project once she had time to do additional research, but that September 11 occurred, and she had not yet had an opportunity to return to the project.

Both IOSs also said they considered assigning the Phoenix project to a headquarters analytic unit but decided against it. In an interview with a supervisory agent in the UBLU, the Joint Inquiry Staff was told that the EC should have been assigned to an analytic unit because it was a long-term, labor-intensive suggestion, and the analytic units would have more time to devote to it then the operational units. There appear to be a number of factors bearing on why the project was not assigned to the analysts that will be discussed later in this statement.

Did FBI Headquarters Management Review the Phoenix EC Prior to September 11?

The chiefs of both the RFU and UBLU informed the Joint Inquiry Staff that they did not see the Phoenix communication prior to September 11. Moreover, neither remembers even hearing about the flight school issue until after September 11. At the

[2] According to documents reviewed by the Joint Inquiry, this individual was not the only pilot with ties to Usama Bin Ladin known to the FBI at that time.

Joint Inquiry Staff's the FBI audited their central records system; the audit supports their statements.

Both the IOSs are unsure, but think they might have mentioned the EC to their unit chiefs prior to September 11. The UBLU IOS said in an interview with the Joint Inquiry Staff that she told her supervisor that Phoenix had sent in a communication about Usama Bin Ladin sending pilots for training and that she planned to do some research before determining what to do about the recommendations in the EC. However, in her interview with the Department of Justice IG in November 2001, she stated that she had not discussed the EC with any supervisory personnel until after the EC was closed. The RFU IOS said she could not recall but might have mentioned the EC to her supervisor in passing.

FBI Headquarters Weaknesses Demonstrated by Handling of Phoenix EC

The manner in which FBI headquarters handled the Phoenix EC provides a valuable window into the FBI's operational environment prior to September 11 and illustrates several procedural weaknesses that have been recognized and are currently being corrected.

The manner in which the Phoenix EC was handled demonstrated how strategic analysis took a back seat to operational priorities prior to September 11. That many in the U.S. Government believed an attack of some type was imminent in the summer of 2001 apparently only served to further de-emphasize strategic analysis. For example, the IOS handling the Phoenix EC was primarily concerned with an individual in the EC who was connected to individuals arrested overseas; the IOS paid less attention to the flight school theories. For his part, the RFU Chief said he was seeing about 100 pieces of mail daily and could not keep up. His solution was to assign the review of intelligence reports to his IOS. Even the analytic unit responsible for strategic analysis was largely producing tactical products to satisfy the operational section. In fact there was no requirement to handle projects with nationwide impact, such as Phoenix, any different than any other project. This has now been changed. Any lead of the type such as Phoenix represented must now be raised to the section chief level.

The handling of the Phoenix EC also exposed information sharing problems between FBI headquarters elements. A number of analysts commented that the UBLU and RFU frequently do not share information with the International Terrorism analytic unit. The supervisor of the UBLU said that the Investigative Services Division, of which the analytic unit is a part, was not a major player and that often information was not shared with it.

Had the project been transferred to the analytic unit the capability to conduct strategic analysis on al-Qa'ida was limited because five of the unit's analysts had transferred into operational units. The Joint Inquiry Staff has been told that every time a competent new analyst arrived, the UBLU or RFU would either try to recruit them as IOSs or would refuse to share information. This allowed the UBLU and RFU to control

the information flow. The end result, unfortunately, is that there is no one left whose role is to perform strategic analysis.

Even if the project had been assigned to the al-Qa'ida analyst in the analytic unit, there can be no guarantee that the various reports about using airplanes as weapons and terrorists sending students to flight school in the United States would have been pieced together. However, there was only one analytic unit at FBI headquarters responsible for counterterrorism, and there were five operational units. It is easier to share information within one unit than it is among five units.

The handling of the Phoenix EC also illustrates the extent to which technological limitations affect information flow at the FBI. A number of individuals who were addressees on the EC have stated that they did not see it prior to September 11. Audits of the system support their statements. The FBI's electronic system is not designed to ensure that all addressees on a communication actually receive it. Instead the electronic version of the document is sent to the unit and then forwarded electronically only to the individual to whom the lead is assigned. Furthermore, the system is capable of recognizing units only if they are precisely designated in the leads section; otherwise, a unit would not receive the communication. In the case of an inaccurate address the communication would be sent into either the Counterterrorism Division's main electronic folder or to the International Terrorism Operations Section's folder where it would sit until the secretaries checked their folders and forwarded it on to the appropriate unit for handling. In fact, the electronic system was considered so unreliable that many FBI personnel, both at the field offices and at FBI headquarters, use email instead. In the case of important communications, they double-check to ensure it is not being neglected. Several FBI personnel interviewed conceded that it was possible that "routine" leads, on which there was no direct communication, were falling through the cracks. RFU and UBLU policies in effect at the time the Phoenix EC was sent gave the person to whom the lead was assigned the discretion to make the determination as to which people in the unit needed to see the report. One person said that he was not certain why the Phoenix agent put all the addressees on the EC but believes the IOS probably made the decision that this was more of an issue for the UBLU and did not need to be routed around to all of the people on the addressee list in the RFU.

The Joint Inquiry Staff has been informed that the FBI recently determined that there are 68,000 outstanding and unassigned leads assigned to the counterterrorism division dating back to 1995. Since many FBI personnel have not been using the electronic system for these purposes, it is difficult to know how many of these leads have actually been completed. The counterterrorism division's management is currently looking into this situation.3

Links from the Phoenix EC to September 11, 2001

3 The Joint Inquiry Staff has asked the FBI for further details and explanation on the status of these outstanding leads, and what actions are being taken to address this situation.

FBI officials have noted, both in public statements and Congressional testimony that the September 11 hijackers did not associate with anyone of investigative interest. However, there is evidence that hijacker Hani Hanjour, who was unknown to the Intelligence Community and law enforcement agencies prior to September 11, 2001, was an associate of an individual mentioned in the Phoenix EC. This individual had been engaged in flight training in the United States, and the FBI believed that he was possibly a radical fundamentalist. The evidence connecting this individual to Hanjour is described below. There are several possible reasons, which will also be discussed below, why this individual's association with Hanjour did not bring Hanjour to the FBI's attention prior to September 11, 2001.

The FBI believes that, beginning in 1997, Hanjour and the individual named in the Phoenix EC trained together at a flight school in Arizona. Several instructors at the flight school say they were associates and one thinks they may have carpooled together. Through various record checks, the FBI has confirmed five occasions when the Phoenix subject and Hanjour were at the flight school on the same day. On one occasion in 1999, the flight school logs indicate that Hanjour and this individual used the same plane. According to the flight instructor, the individual mentioned in the Phoenix EC was there as an observer. The rules of the flight school were such that for this individual to observe, Hanjour would have had to approve of his presence in the aircraft. Another individual informed the FBI after September 11, 2001 that this individual and Hanjour knew each other, both from flight training and through a religious center in Arizona.

The FBI's evidence linking the two in the summer of 2001 is not as strong. The FBI has located records from a flight school in Phoenix indicating that on one day in June 2001, Hanjour and several other individuals signed up to use the Cessna simulator. The next day, the two individuals who signed up with Hanjour the previous day, came to the facility with the individual mentioned in the Phoenix EC. An employee of the flight school has informed the FBI that he recalls a fourth individual being there with him but cannot remember who. Another employee of the flight school has placed Hanjour and this individual together during that time frame, although she was not completely confident in her identification.

The FBI attempted to investigate this individual in May 2001, but discovered that he was out of the country. The FBI was apparently unaware that he returned to the United States soon after, and may have been associating with Hanjour and several other Islamic extremists. 4 A Phoenix agent told the JIS that had the individual been in the country in May 2001, they would have opened an investigation. However, the Phoenix office generally did not open investigations on individuals whom they believed had permanently left the United States. Although there were no legal bars to opening an

4 The Joint Inquiry Staff is still attempting to determine whether the FBI's Phoenix office was aware of this individual's presence in the United States in the summer of 2001. The JIS has interviewed three agents in Phoenix about this issue, and received slightly contradictory answers. The JIS has asked the FBI for clarification on this issue.

investigation, FBIHQ discouraged this practice. The Phoenix office also did not notify the INS, State Department, or the CIA of their interest in this individual.

No one can say whether the FBI would have developed an investigative interest in Hanjour had they opened an investigation on the individual mentioned in the Phoenix EC prior to September 11, 2001. The Joint Inquiry Staff is also not suggesting that if they had, it would have necessarily led to the discovery of the September 11 plot. However, this example provides additional evidence that at least some of the hijackers may have been less isolated and more integrated into their communities than was previously thought. If the hijackers were, in fact, associating with individuals of investigative interest, and were not keeping to themselves as has been portrayed, there are more significant questions as to whether or not they should have come to the FBI's attention prior to the attacks. These associations continue to raise questions about the FBI's knowledge and understanding of the radical fundamentalist network in the United States prior to September 11, 2001.

This case also raises questions about the FBI's policy and practice prior to September 11, 2001 regarding the initiation of investigations on individuals outside of the United States. The Phoenix FBI agent noted that this policy and practice have since been changed. It also provides a valuable illustration of how crucial it is for the FBI to coordinate its investigations internally and with other U.S. Government agencies, particularly when individuals are traveling into and out of the United States.

For this system to work effectively, and for the FBI to be aware when individuals of previous investigative interest return to the United States, they have to have close contact with INS and CIA. Unfortunately, it appears that prior to September 11, 2001, there was no system in place to ensure coordination. In this case, the FBI did not notify the INS, State Department, or the CIA of their interest in the Phoenix subject. Therefore, this individual was able to get into the United States without any notification to the FBI that he had returned. Supposedly coordination with INS and CIA is much better now, and the FBI does a better job of notification to those agencies.

Finally, the Phoenix subject's name was not provided to the TIPOFF watchlist at the State Department nor to the NAILS watchlist at INS. The individual's name and information regarding his terrorist associations and background were provided to the TIPOFF program by the FBI and the CIA after the September 11 attacks. It is only by identifying this individual to the TIPOFF and NAILS watchlist that the FBI could have been assured that he would be kept out of the United States.

Previous FBI Focus at U.S. Flight Schools

The Phoenix EC was not the first occasion that the FBI had been concerned about terrorist groups sending individuals to the United States for aviation study. The EC should be understood in this broader context. It is also important to note that the neither individuals involved in drafting the Phoenix EC nor the FBI personnel who worked on it at FBI headquarters were aware of this broader context.

In 1981, the U.S. military was involved in hostilities with the Libyan Air Force in the Gulf of Sidra. President Reagan made the decision to deport all Libyan students in the United States involved in either aviation or nuclear studies. In March 1983, the INS published a rule in the Federal Register, terminating the nonimmigrant status of Libyan nationals or individuals acting on behalf of Libyan entities engaged in aviation- or nuclear-related education. The INS turned to the FBI for assistance in locating any such individuals. On May 6, 1983, FBI headquarters sent a "priority" communication to all field offices, asking the field offices for assistance in complying with the INS request. The Joint Inquiry Staff has not been able to locate all of the relevant records, so it is not clear how many students the FBI located and deported.

In 1998, the Chief Pilot of the FBI's Oklahoma City Field Office contacted an agent on the office's counterterrorism squad to inform him that he had observed a large numbers of Middle Eastern males at Oklahoma flight schools. An intra-office communication to the counterterrorism squad supervisor was drafted noting the Chief Pilot's concern that the aviation education might be related to planned terrorist activity, and his speculation that light planes would be an ideal means of spreading chemical or biological agents. The communication was sent to the office's "Weapons of Mass Destruction" control file. It appears to have been for informational purposes only. There is no indication that any follow-up action was either requested or conducted.

The FBI received reporting in 1998 that a terrorist organization might be planning to bring students to the United States for training at a flight school. The FBI was aware that individuals connected to the organization had performed surveillance and security tests at airports in the United States and made comments suggesting an intention to target civil aviation. There is no indication that this organization actually followed through on their plans.

In 1999, reporting was received that yet another terrorist organization was planning to send students to the United States for aviation training. The purpose of this training was unknown, but the terrorist organization leaders viewed the requirement as being "particularly important" and were reported to have approved an open-ended amount of funding to ensure its success. In response, an operational unit in the Counterterrorism Section at FBI headquarters sent a communication to 24 field offices, asking them to pay close attention to Islamic students in their area from the target country who were engaged in aviation training. This communication was sent to the Phoenix Office's International Terrorism squad, but the Phoenix SA does not recall this reporting. The Phoenix SSA was not assigned to the Phoenix Office at the time.

The communication requested that field offices "task sources, coordinate with the INS, and conduct other logical inquiries, in an effort to develop an intelligence baseline" regarding this terrorist group's use of students. To this point, there is no indication that the FBI field offices conducted any investigation after receiving the communication. The analyst who drafted the communication indicated that he did receive several calls from field offices, but that the calls were either to seek additional guidance or to raise concerns

about the Buckley Amendment implications of investigating at schools. (The Buckley Amendment is part of the 1974 Family Educational Rights and Privacy Act, which bars post secondary educational institutions which receive federal funding from releasing students' personal information without their written consent.)

In November 1999, to address these concerns, the FBI sent a letter to INS explaining the intelligence and requesting a database search for individuals studying in the United States from the target country. Any information provided by the INS would be sent to the field offices, which would conduct appropriate investigations in coordination with local INS agents. According to interviews, the INS never provided any information in response to the request.

The project was subsequently assigned to the International Terrorism Analytic Unit at FBI headquarters. The analyst assigned to the project determined that there were 75 academic institutions offering flight education in the United States. He also located, via the Internet, an additional 1000 flight schools. In November 2000, the analyst sent a communication to the FBI field offices, informing them that no information was uncovered concerning this terrorist group's recruitment of students studying aviation and stated that "further investigation by FBI field offices is deemed imprudent" by FBI headquarters.

The former unit chief of the operational unit involved in this project told the Joint Inquiry Staff that he was not surprised by the apparent lack of vigorous investigative action by the field offices. He believes that the field offices' calls requesting additional guidance or raising Buckley Amendment issues were just "excuses" and that the field offices should have known full well how to go about this effort. In his view, this type of project was like "drilling for oil," in that you drill in many different spots, almost all of which are unsuccessful but the reward from one successful "drilling" is worth the effort. In his opinion, the field offices did not like to undertake difficult labor-intensive projects like this with a high risk of failure. The FBI's culture often prevented headquarters from forcing field offices to take investigative action that they were unwilling to take. He told us that the FBI was so decentralized, and the Special Agents in Charge wielded such power, that when field agents complained to a supervisor about a request from headquarters, FBI headquarters management would generally back down.

Missed Opportunity to Connect Phoenix to Similar Investigations?

The personnel working on the Phoenix EC at FBI headquarters were not aware of the prior reporting on terrorist groups sending aviation students to the United States and did not know that FBI headquarters had undertaken a systematic effort in 1999 to identify Middle Eastern flight students in the United States. This is not surprising considering the lack of information sharing in the FBI. According to interviewees, this is a problem not only at FBI headquarters but at the field offices as well. Agents often will only be familiar with cases on their own squad and will not know about investigations on other squads.

Had the headquarters personnel working on the Phoenix EC known about the 1999 efforts by FBI headquarters to locate foreign nationals at flight schools, it might have affected how they handled the EC. The IOSs handling the EC were concerned about the legal implications of following through on the recommendations but were unaware of similar efforts in the past whereby the INS and FBI had established an arrangement to provide the FBI with foreign nationals' student visas for investigative purposes. Unfortunately, instead of approaching FBI lawyers to determine whether there were legal obstacles to implementation, the IOSs decided among themselves that the EC raised profiling issues.

This lack of information sharing among personnel working different targets poses increasing problems for the FBI faced with a national security environment and the growth of the "International Jihad" movement, making it difficult to link individuals to specific foreign powers or terrorist groups. Some FBI personnel expressed concern that the FBI's labeling of individuals as associated with particular terrorist organizations is not always accurate. For example, an individual affiliated with al-Qa'ida may associate with Hamas members in the United States and be labeled Hamas based on these associations. If such an individual is being worked out of another unit, the traditional lack of information sharing makes it unlikely the al-Qa'ida unit will learn about the investigation. This affects the unit's ability to develop a comprehensive understanding of al-Qa'ida presence and operations in the United States. There may also be al- Qa'ida information directly relevant to the investigation about which personnel working Hamas are unaware.

New York FBI Office Actions in Connection with the Phoenix EC

The Phoenix EC was sent to two investigators in the FBI's New York field office who specialize in Usama Bin Ladin cases. They were asked to "read and clear" but were not asked to take any follow-up action. A Joint Inquiry Staff audit of electronic records shows that at least three people in New York saw the EC prior to September 11. It does not appear to have received much attention or elicited concern. Two of the three do not recall the communication prior to September 11, 2001. The third remembered reading it but said it did not resonate with him because he found it speculative.

The New York agents interviewed stated that they were well aware that Middle Eastern men frequently came to the United States for flight training. This was not surprising as it was considered the best and most reasonably priced place to train. According to them, many foreign nationals got their commercial flight training here.

A communication noting that Middle Eastern men with ties to Usama Bin Ladin were receiving flight training in the United States would not necessarily be considered particularly alarming because New York personnel knew that individuals connected to al-Qa'ida had previously received flight training in the United States. In fact, one of these individuals trained at the Airman Flight School in Norman, Oklahoma, the same place where Zacarias Moussaoui trained prior to his arrival in Minnesota. Mohammed Atta and another of the hijackers visited this same flight school but decided not to enroll there.

The commonly held view at the FBI prior to September 11 was that Bin Ladin needed pilots to operate aircraft he had purchased in the United States to move men and material. Also, several pilots with al-Qa'ida ties testified for the U.S. Government during the course of the Embassy bombing trial.

However, the FBI had also received reporting that was not entirely consistent with this view of Usama Bin Ladin's pilots. Two of the pilots had been through al Qa'ida training camps in Afghanistan where they were trained to conduct terrorist operations. One of them was trained in surveillance and intelligence, apparently being selected for the course due to his aviation skills.

The FBI also received reporting that, in 1994, individuals with terrorist connections had requested and received training in the technical aspects of aviation including instruction on takeoff and landing procedures, approach altitudes, and aircraft identification methods. They stated that they would be passing on the information to other individuals with terrorist connections, but did not mention any specific plan. The FBI disseminated the information to the FAA, the State Department, and the CIA.

The FBI Investigation of Zacarias Moussaoui, August 16 to September 11, 2001

Zacarias Moussaoui came to the attention of the FBI during a period of time when the Intelligence Community was detecting numerous indicators of an impending terrorist attack against U.S. interests somewhere in the world. Moussaoui was in the custody of the INS on September 11, 2001. Our review has, in part, focused on whether information resulting from the FBI's investigation of Moussaoui could have alerted the U.S. Government to the scope and nature of the attacks that occurred on September 11, 2001.

Moussaoui has been indicted and faces a criminal trial this fall. In order to avoid affecting the course of that proceeding, the Joint Inquiry Staff **originally** limited the amount of detail in this presentation while attempting to provide a general understanding of the facts of the investigation. **Consistent with a September 23, 2002 order of the Court in the Moussaoui case that clarified the nature of the information that could be discussed in public, additional information has been included in this version of the Statement.**

Our review of the FBI's investigation to date has identified three issues in particular, to which I would draw Members' attention:

- Differences in the way the FBI's field offices and headquarters components analyzed and perceived the danger posed by the facts uncovered during the FBI's investigation of Moussaoui prior to September 11, 2001;

- The tools available to the FBI under the Constitution and laws of the United States to investigate that danger, notably the Foreign Intelligence Surveillance Act

(FISA), and whether FBI personnel were well organized and informed about the availability of those tools; and

- Whether the substance, clarity, and urgency of the threat warning provided by the FBI to other parts of the Intelligence Community corresponded to the danger that had been identified.

For purposes of this interim report, the American public should understand that, under FISA, the FBI can obtain a court order authorizing a physical search or electronic surveillance, such as a wiretap, if it can demonstrate that the subject: (1) is an agent of a foreign power, which can be a foreign country or an international terrorist group, and (2) was, among other things, engaged in international terrorism, or activities in preparation therefor, on behalf of that foreign power. Court orders issued under FISA are classified and are issued by the Foreign Intelligence Surveillance Court (FISC).

The FBI's focus at the time Moussaoui was taken into custody appears to the Joint Inquiry Staff to have been almost entirely on investigating specific crimes and not on identifying linkages between separate investigations or on sharing information with other U.S. Government agencies with counterterrorist responsibilities. No one at FBI headquarters apparently connected Moussaoui, the Phoenix memo, the possible presence of Khalid al-Mihdhar and Nawaf al-Hazmi in the United States, or the flood of warnings about possible terrorist attacks during the summer of 2001.

From interviews with flight school personnel and with Moussaoui himself in August 2001, the FBI pieced together the details of Moussaoui's arrival in the United States. Moussaoui had contacted the Airman Flight School by email on September 29, 2000 and expressed interest in taking lessons to fly a small Cessna aircraft. On February 23, 2001, he entered the United States at Chicago's O'Hare Airport. He was traveling on a French passport and this allowed him to stay in the country without a visa for 90 days, until May 22, 2001. On February 26, 2001, he began flight lessons at Airman Flight School.

Moussaoui was unhappy with the training at Airman and, at the end of May 2001, had contacted Pan American International Flight School in Minneapolis. While Airman Flight School provided flight lessons in piloting Cessnas and similar small aircraft, Pan Am provided ground training and access to a Boeing 747 flight simulator used by professional pilots.

Most of Pan Am's students are either newly hired airline pilots who use the flight simulator for initial training or are active airline pilots who use the equipment for an update or refresher training. Although anyone can sign up for lessons at Pan Am, the typical student has a pilot's license, is employed by an airline, and has several thousand flight hours. Moussaoui had none of these qualifications.

On August 11, 2001, Moussaoui and his roommate, Hussein al-Attas, arrived in Egan, Minnesota and checked into a hotel. Moussaoui began classes at Pan Am on

August 13, 2001. **On Wednesday, August 15, 2001, an employee at Pan Am called the FBI's Minneapolis Field Office because the employee and other Pan Am employees were suspicious of Moussaoui.**

The FBI determined that Moussaoui had paid $8,000 to $9,000 in cash for training on the Boeing 747 Model 400 aircraft simulator but met none of the usual criteria for students at the flight school. What set Moussaoui apart from all other students was that Moussaoui had no aviation background and, apparently, no pilot's license. It was also considered odd that Moussaoui indicated that he wished to learn to take off and land the 747 Model 400, which he referred to as an "ego boosting thing." It should be noted that this conflicts with published reports that he only wanted to pilot the plane in the air and did not want to land or take off.

Based on the information from the flight school, the FBI's Minneapolis Field Office opened an international terrorism investigation of Moussaoui. **The Minneapolis Field Office reportedly viewed Moussaoui as a threat to national security.**

The FBI's Minneapolis Field Office hosts and is part of a Joint Terrorism Task Force, or JTTF. Agents of the INS share space and work closely with the FBI in Minneapolis and were able to immediately determine that Moussaoui had been authorized to stay in the United States only until May 22, 2001. Thus, Moussaoui was "out of status" at the time – August – that the FBI began investigating him.

On the same day the Minneapolis field office learned about Moussaoui, it asked both the CIA and the FBI's legal attaché in Paris for any information they had or could get on Moussaoui. At the same time, they also informed FBI headquarters of the investigation. The supervisory agent in Minneapolis told the Joint Inquiry Staff that FBI headquarters had suggested that Moussaoui be put under surveillance, but that Minneapolis did not have enough agents to do that. Furthermore, the Minneapolis agents believed that it was more important to prevent Moussaoui from getting any additional flight training.

On Thursday, August 16, the FBI determined that Moussaoui was unlike any other student with whom his flight instructor had worked. Moussaoui began the ground school portion of the training with instruction in aircraft systems using a Power Point presentation. This portion of the instruction reportedly was useless for Moussaoui, who had no background in any type of sophisticated aircraft systems and, apparently, had only approximately 50 hours of flight training in light civil aircraft bearing no similarity to the 747-400. In addition, Moussaoui was extremely interested in the operation of the plane's doors and control panel, which Pan Am found suspicious. Further, Moussaoui reportedly said that he would "love" to fly a simulated flight from Heathrow Airport in England to John F. Kennedy Airport in New York. Moussaoui seemed to have a legitimate interest in aircraft and had asked for recommendations for schools to provide subsequent training.

After **conducting flight school interviews**, the FBI agents, along with two INS agents, went to Moussaoui's hotel. The INS agents temporarily detained Moussaoui and his roommate, Hussein al-Attas, while checking to determine if they were legally in the United States. Al-Attas showed the INS that he had a valid student visa and agreed to allow the agents to search his property in the hotel room.[5]

Moussaoui showed the agents his passport case, which included his passport, a British driver's license, a bank statement showing a deposit of $32,000 in cash to an Oklahoma account, and an application to extend his stay in the United States. The INS agents determined that Moussaoui had not received an extension to allow him to stay in the United States beyond May 22, 2001, so they took him into custody.

Moussaoui declined to allow the agents to search his belongings. When the agents told Moussaoui that he would be deported, Moussaoui agreed to let the agents take his belongings to the INS office for safekeeping. The agents packed Moussaoui's belongings, noticing that he had a laptop computer among his possessions.

The agents interviewed Moussaoui at the INS office in Minneapolis. Moussaoui told them that he had traveled to Morocco, Malaysia, and Pakistan for business, although he could not provide any details of his employment. Nor could he convincingly explain the $32,000 bank balance.

After Moussaoui's detention, the Minneapolis supervisory agent called the office's legal counsel and asked if there was any way to search Moussaoui's possessions without his consent. He was told he had to obtain a search warrant.

Over the ensuing days, the Minneapolis agents considered several alternatives, including trying to obtain a criminal search warrant, seeking a search warrant under FISA, and deporting Moussaoui to France after arranging for the French authorities to search Moussaoui's possessions and share their findings with the FBI. Adding to the sense of urgency, a supervisor in the INS' Minneapolis office told the FBI that INS typically does not hold visa waiver violators like Moussaoui for more than 24 hours before returning them to their home countries. Under the circumstances, however, the INS said it would hold Moussaoui for seven to ten days.

The FBI conducted no additional interviews of Moussaoui after August 17, 2001. On Saturday, August 18, Minneapolis sent a detailed memorandum to FBI headquarters describing the Moussaoui investigation and stating that, **based on Moussaoui's "possession of weapons and his preparation through physical training for violent confrontation," Minneapolis had reason to believe that Moussaoui, al-Attas "and others yet unknown" were conspiring to seize control of an airplane.**

The Joint Inquiry Staff has been told in interviews with the Minneapolis agents that FBI headquarters advised against trying to obtain a criminal search warrant as that

---

5 Al-Attas was recently convicted of making false statements to the FBI regarding statements by Moussaoui and the extent of his relationship with Moussaoui. He remains in custody as a material witness.

might prejudice any subsequent efforts to get a search warrant under FISA. Under FISA, a search warrant could be obtained if they could show there was probable cause to believe Moussaoui was an agent of a foreign power and either engaged in terrorism or was preparing to engage in terrorism. FBI headquarters was concerned that if a criminal warrant was denied and then the agents tried to get a warrant under FISA, the court would think the agents were trying to use authority for an intelligence investigation to pursue a criminal case.

During this time frame an attorney in the National Security Law Unit at FBI headquarters asked the counsel in the Minneapolis field office if she had considered trying to obtain a criminal warrant and she replied that a FISA warrant would be the safer course. Minneapolis also wanted to notify the Criminal Division about Moussaoui through the local U.S. Attorney's Office, believing it was obligated to do so under Attorney General guidelines that required notification when there is a "reasonable indication" of a felony. FBI headquarters advised that Minneapolis did not have enough evidence to warrant notifying the Criminal Division.

The FBI case agent in Minneapolis had become increasingly frustrated with what he perceived as a lack of assistance from the Radical Fundamentalist Unit (RFU) at FBI headquarters. He had had previous conflicts with the RFU agent over FISA issues and believed headquarters was not being responsive to the threat Minneapolis had identified. At the suggestion of a Minneapolis supervisor, the Minneapolis case agent contacted an FBI official who was detailed to the CTC. The Minneapolis agent shared the details of the Moussaoui investigation with him and provided the names of associates that had been connected to Moussaoui. The Minneapolis case agent has told the Joint Inquiry Staff that he was looking for any information that CTC could provide that would strengthen the case linking Moussaoui to international terrorism.

On August 21, 2001, the Minneapolis case agent sent an email to the supervisory special agent in the RFU who was handling this matter, stating: **"[It's] imperative that the** [U.S. Secret Service] be apprised of this threat potential **indicated by the evidence... If [Moussaoui] seizes an aircraft flying from Heathrow to NYC, it will have the fuel on board to reach DC."** In an interview with the Joint Inquiry Staff, the RFU agent to whom the message was addressed said that he told the Minneapolis agent that he was working on a notification to the entire Intelligence Community, including the Secret Service, about the threat presented by Moussaoui.

The RFU supervisory special agent sent a teletype on September 4, 2001, recounting the FBI's interviews of Moussaoui and al-Attas, and other information it had obtained in the meantime. The teletype, however, merely recounted the steps in the investigation. It did not place Moussaoui's actions in the context of the increased level of terrorist threats during the summer of 2001, nor did it provide its recipients with any analysis of Moussaoui's actions or plans, or information about what type of threat he may have presented.

A CIA officer detailed to FBI headquarters learned of the Moussaoui investigation from CTC in the third week of August 2001. The officer was alarmed about Moussaoui for several reasons. **First, Moussaoui had denied being a Muslim to the flight instructor, while al-Attas (Moussaoui's companion at the flight school) informed the FBI that Moussaoui was a fundamentalist. Further, the fact Moussaoui was interested in using the Minneapolis flight school simulator to learn to fly from Heathrow to JFK Airport, made him concerned that Moussaoui was a hijacker. Others were similarly concerned.** CIA stations were advised of the know facts regarding Moussaoui and al-Attas and were asked to provide any relevant information they might have. **The two were described as "suspect 747 airline attackers" and "suspect airline suicide attacker," who might be "involved in a larger plot to target airlines traveling from Europe to the U.S...."**

On Wednesday, August 22, the FBI legal attache's office in Paris provided its report. That report started a series of discussions between Minneapolis and the RFU at FBI headquarters focusing on whether a specific group of Chechen rebels was a "recognized" foreign power, i.e., one that was on the State Department's list of terrorist groups and for which the Foreign Intelligence Surveillance Court had previously granted orders. The RFU agent believed that the Chechen rebels were not a "recognized" foreign power and that, even if Moussaoui were to be linked to them, the FBI could not obtain a search order under FISA. Thus, the RFU agent told the Minneapolis agents that they needed to somehow connect Moussaoui to al-Qa'ida, which he believed was a "recognized" foreign power. This led the Minneapolis agents to attempt to gather information showing that the Chechen rebels were connected to al-Qa'ida.

Unfortunately this dialogue was based on a misunderstanding of FISA. The FBI's Deputy General Counsel told the Joint Inquiry Staff that the term "recognized foreign power" has no meaning under FISA and that the FBI can obtain a search warrant under FISA for an agent of <u>any</u> international terrorist group, including the Chechen rebels. But because of the misunderstanding Minneapolis spent the better part of three weeks trying to connect the Chechen group to al-Qa'ida. The Minneapolis case agent contacted CTC, asking for additional information concerning connections between the group and al-Qa'ida; he also suggested that the RFU agent contact CTC for assistance on the issue. The RFU agent responded that he had all the information he needed and requested that Minneapolis work through FBI headquarters when contacting CTC. Ultimately, the RFU agent agreed to submit Minneapolis' FISA request to the attorneys in the FBI's National Security Law Unit (NSLU) for review.

The Joint Inquiry Staff interviewed several FBI attorneys with whom the RFU agent consulted about Moussaoui. All have confirmed that they advised the RFU agent that the evidence was insufficient to link Moussaoui to a foreign power. One of the attorneys also told the RFU agent that the Chechen rebels were not a "recognized" foreign power. The attorneys also told the Staff that, if they had been aware of the Phoenix memo, they would have forwarded the FISA request to the Justice Department's Office of Intelligence Policy Review (OIPR). They reasoned that the particulars of the

Phoenix memo changed the context of the Moussaoui investigation and made a stronger case for the FISA warrant. None of them saw the Phoenix memo before September 11.

Two FBI agents assigned to the Oklahoma City Field Office's international terrorism squad visited Airman Flight School in Norman, Oklahoma on August 23. In September of 1999, one of the agents had been assigned a lead from the Orlando Field Office to visit the flight school concerning another individual, who had been identified as Usama Bin Ladin's personal pilot and who had received flight training at Airman. The agent had not been given any background information about this individual; he did not know that this individual had cooperated with the FBI during the Embassy Bombings trial. Although he told us that he thought that this lead had been the most significant information he had seen in Oklahoma City, the agent did not remember the lead when he returned to the flight school two years later to ask questions about Moussaoui. He told the Joint Inquiry Staff that he should have connected the two visits but that he did not have the time to do so.

During a conversation on August 27, 2001, the RFU agent told the Minneapolis supervisor that the supervisor was getting people "spun up" over Moussaoui. According to his notes and his statement to the Joint Inquiry Staff, the supervisor replied that he was trying to get people at FBI headquarters "spun up" because he was trying to make sure that Moussaoui "did not take control of a plane and fly it into the World Trade Center." The Minneapolis agent said that the headquarters agent told him, "[T]hat's not going to happen. We don't know he's a terrorist. You don't have enough to show he is a terrorist. You have a guy interested in this type of aircraft – that is it." The headquarters agent does not remember this exchange. The Minneapolis supervisor told the Joint Inquiry Staff that he had no reason to believe that Moussaoui was planning an attack on the World Trade Center; he was merely trying to get headquarters' attention.

In a subsequent conference call with FBI headquarters, the chief of the RFU Unit told Minneapolis that a connection with a specific recognized foreign power, such as HAMAS, was necessary to get a FISA search warrant.

On August 28, 2001, after reviewing the request for a search warrant, the RFU agent edited it and returned the request to Minneapolis for comment. The RFU agent says that it was not unusual for headquarters agents to make changes to field submissions in addition to changes made by the NSLU and OIPR. The major substantive change that was made was the removal of information about connections between the Chechen rebels and al-Qa'ida. The RFU agent said he removed it because he believed this information was insufficient and that, if he received approval from the NSLU to use the Chechen rebels as a foreign power, he would have added it back to an expanded section about Chechnya.

After the edit was complete, the RFU agent briefed the FBI Deputy General Counsel. The Deputy General Counsel told the Joint Inquiry Staff that he agreed with the RFU agent that there was insufficient information to show that Moussaoui was an agent of a foreign power, but that the issue of a "recognized" foreign power did not come

up. After that briefing, the RFU agent sent an email to Minneapolis saying that the information was even less sufficient than he had previously thought because Moussaoui would actually have to be shown to be a part of a movement or organization.

Subsequent to concluding that there was insufficient information to show that Moussaoui was an agent of any foreign power, the FBI's focus shifted to arranging for Moussaoui's planned deportation to France on September 17. French officials would search his belongings and provide the results to the FBI. Although the FBI was no longer considering a search warrant under FISA, no one revisited the idea of attempting to obtain a criminal search warrant, even though the only reason for not attempting to obtain a criminal search warrant – the concern that it would prejudice a request under FISA – no longer existed.

On Thursday, September 4, 2001, FBI headquarters sent a teletype to the Intelligence Community and other U.S. Government agencies, including the Federal Aviation Administration (FAA), providing information about the Moussaoui investigation. The teletype noted that Moussaoui was being held in custody but did not describe any particular threat that the FBI thought he posed, for example, whether he might be connected to a larger plot. The teletype also did not recommend that the addressees take any action or look for any additional indicators of a terrorist attack, nor did it provide any analysis of a possible hijacking threat or provide any specific warnings. The following day the Minneapolis case agent hand-carried the teletype to two employees of the FAA's Bloomington, Minnesota office and orally briefed them on the status of the investigation. The two FAA employees told the Joint Inquiry Staff that the FBI agent did not convey any sense of urgency about the teletype and did not ask them to take any specific action regarding Moussaoui. He just wanted to be sure the FAA had received the cable.

The final preparations for Moussaoui's deportation were underway when the September 11 attacks occurred.

Prior to September 11, 2001, no one at the FBI canvassed other individuals in the custody of and cooperating with the U.S. Government in connection with past terrorism cases to see if any of those individuals knew Moussaoui.

Conclusion

The staff has described three series of events – pertaining to al-Mihdhar and al-Hazmi, the Phoenix EC, and Zacarias Moussaoui – each of which raises significant questions in their own right. In the wake of the September 11 attacks, they also illustrate the danger of seeing events in isolation from each other. In our view, taken together, they clearly demonstrate how our counterterrorist efforts must be based on a comprehensive and current understanding of the overall context in which terrorist networks like al-Qa'ida operate.

The first matter involved Khalid al-Mihdhar and Nawaf al-Hazmi, the two hijackers who came to the attention of the Intelligence Community in early 2000 but subsequently entered the United States unobserved and undetected later. The Intelligence Community succeeded in determining that these Bin Laden operatives were traveling in January 2000 to Malaysia and in collecting important information about them. The system broke down, however, in making the best use of that information and in ensuring that it was effectively and fully shared with agencies, like the FBI, the State Department and the INS, that could have acted on it to either prevent them from entering the United States or surveil them and uncover their activities while in the United States.

In addition, the FBI and the CIA had responsibilities to respond to the October 2000 attack on *USS Cole*. Each had information that the other needed to carry out those responsibilities. But, at a key meeting in New York on June 11, 2001, the CIA did not provide to the FBI information about the Malaysian meeting and its participants that could have assisted the FBI in its investigation. These events reflect misunderstandings that have developed over the last several years about the use of information derived from intelligence gathering activities in criminal investigations.

The problem of communication demonstrated by the al-Mihdhar/al-Hazmi story existed not only between the CIA and FBI, but also within the FBI itself. Once it was determined in late August 2001 that Khalid al-Mihdhar was in the United States, the search to determine his whereabouts was constrained by FBI policies and practices regarding the use of intelligence information in FBI criminal investigations. This limited the resources that were made available for the FBI to conduct the search during a time in which al-Mihdhar and al-Hazmi were purchasing their September 11 tickets and traveling to their last rallying points.

The second matter – the Phoenix EC – also illustrates the Intelligence Community's strength and weaknesses. An FBI field agent perceived, amidst a profusion of cases, that terrorists could use the well-developed system of flight training education in the United States to prepare an attack against us. The field agent understood that it was necessary to go beyond individual cases and to undertake an empirical analysis broader than the geographic limits of a single field office. The idea was submitted to FBI headquarters, where, for a variety of reasons, it generated almost no interest. First, no one gleaned from the FBI's own records that others at the Bureau had previously expressed concerns about possible terrorists at U.S. flight education institutions. Second, anticipating future threats has not been a significant part of the FBI's general approach to its work. Third, the highest levels of the Intelligence Community had not communicated effectively to its personnel the critical importance of analyzing information in light of the growing awareness of an impending terrorist attack in the summer of 2001. Finally, FBI management did not perceive it would be useful to simply alert others at the FBI to the danger that one of its field offices perceived.

As for the third matter, one can see in the pre-September 11 handling of the case of Zacarias Moussaoui a myopic focus within both the FBI and the DCI's CTC on the case at hand. An FBI field agent and his supervisor saw a potential threat, were

concerned about the possibility of a larger plot to target airlines, and reported their concerns to FBI headquarters. The Moussaoui information was also shared with the DCI's CTC. But, neither FBI headquarters nor the DCI's CTC linked this information to warnings emanating from the CTC in the summer of 2001 about an impending terrorist attack, nor did they see a possible connection to information available on August 23, 2001 that Bin Ladin operatives had entered the United States. The same unit at FBI headquarters also had the Phoenix EC, but still did not sound any alarm bells.

No one will ever know whether a greater focus on the connection between these events would have led to the unraveling of the September 11 plot. But, clearly, it might have drawn greater attention to the possibility of a terrorist attack in the United States, generated a heightened state of alert regarding such attacks, and prompted more aggressive investigation and intelligence gathering regarding the information our Government did possess prior to September 11.

Mr. Chairman, members of these two Committees, this completes my statement for today's hearing. Thank you.

[The prepared statement of Ms. Hill follows:]

Joint Inquiry Staff Statement
Eleanor Hill, Staff Director
October 17, 2002

Introduction

Chairman Goss, Chairman Graham, members of this Joint Inquiry, good morning. Over the course of the last few months, these Committees have considered a great deal of information, obtained both through witness testimony and documentary review. This morning's testimony by the senior leadership of the Intelligence Community will bring to a close this series of open hearings. What has been perhaps unprecedented, at least in terms of the Intelligence Committees, is the extent to which a good portion of this review has been accomplished through open, public hearings. That effort was driven by both the magnitude of September 11th and your recognition of the American public's need to better understand the performance of their government, and particularly the Intelligence Community, with respect to the events of that day.

Beyond the events of September 11th, however, we believe these open hearings have also served to educate the public on the ongoing policy debate about the future path of the Intelligence Community. The considerable factual record that is now before these Committees touches on a wide range of issues that are critical to that debate. Ultimately, many of those issues will be considered and addressed in even greater depth as these Committees deliberate on what will become the final report of this Joint Inquiry. At this point, however, the Staff has been asked to briefly review the most important elements of the factual record as well as key questions that we believe have been raised through the course of these public hearings.

Review of Key Facts

Beginning with the initial public hearing, the record describes, in considerable detail, the situation confronting the U. S. Intelligence Community with respect to the terrorist threat posed by Usama Bin Ladin prior to September 11, 2001. Key facts include:

- Usama Bin Ladin's public *fatwa* in 1998 authorizing terrorist attacks against American civilians and military personnel worldwide;

- Information acquired by the Intelligence Community over a three-year period indicating in broad terms that Usama Bin Ladin's network intended to carry out attacks inside the United States;

- The Director of Central Intelligence's (DCI) statement in December 1998 that "we are at war" with Usama Bin Ladin and that no resources should be spared by the Intelligence Community in that regard;

- Information accumulated by the Intelligence Community over the course of a seven-year period indicating that international terrorists had considered using airplanes as weapons; and

- Numerous indicators of a major impending terrorist attack detected by the Intelligence Community in the spring and summer of 2001. Although those indicators lacked the specifics of precisely where, when, or how the attack would occur, the Intelligence Community had information indicating that the attack was likely to have dramatic consequences for governments and cause mass casualties.

While the specifics of the September 11th attacks were not known in advance, relevant information was available in the summer of 2001. The collective significance of that information was not, however, recognized. Perhaps as a result, the information was not fully shared, in a timely and effective manner, both within the Intelligence Community and with other federal agencies. Examples include:

- In January 2000, the Central Intelligence Agency (CIA) succeeded in determining that Bin Laden operatives Khalid al-Mihdhar and Nawaf al-Hazmi were in Malaysia and in obtaining important information about them. While some information regarding the two was provided to the FBI at an early point, the weight of the evidence suggests that the CIA apparently did not transmit information regarding al-Mihdhar's possession of a U.S. multiple-entry visa and the likelihood of travel by al-Mihdhar, and later by al-Hazmi, to the United States, despite various opportunities to do so in January 2000, March 2000, and June 2001;

- It was not until late August 2001 that the CIA watch-listed al-Mihdhar and al-Hazmi and advised the FBI of their likely presence in the United States. FBI efforts to locate them through the New York and Los Angeles FBI offices proved unsuccessful. Other potentially useful federal agencies were apparently not fully enlisted in that effort: representatives of the State Department, the FAA, and the INS all testified that, prior to September 11th, their agencies were not asked to utilize their own information databases as part of the effort to find al-Mihdhar and al-Hazmi. An FAA representative, for example, testified that he believes that, had the FAA been given the names of the two individuals, they would have "picked them up in the reservations system";

- The FBI did not grasp the significance of a July 2001 electronic communication from the Phoenix field office identifying a pattern of Middle Eastern males with possible terrorist connections attending flight schools in the United States. Apparently no one at FBI headquarters connected that idea to previous FBI concerns about the topic or to the increasing threat of a terrorist attack in the summer of 2001. The communication generated no broader analytic effort on the issue nor any special alert within the Intelligence Community. Despite its relevance to civil aviation, the FAA did not receive the communication until it was brought to the agency's attention in 2002 by the Joint Inquiry Staff;

- Also in the summer of 2001, agents in an FBI field office saw in Zacarias Moussaoui a potential terrorist threat, were concerned about the possibility of a larger plot to target airlines, and shared those concerns with both FBI headquarters and the DCI's Counterterrorism Center. Neither FBI headquarters nor the CTC apparently connected the information to warnings emanating from the CTC about an impending terrorist attack or to the likely presence of two al-Qa'ida operatives, al-Mihdhar and al-Hazmi, in the United States. The same unit at FBI headquarters handled the Phoenix EC, but still did not sound any alarm bells.

No one will ever know whether more extensive analytic efforts, fuller and more timely information sharing, or a greater focus on the connection between these events would have led to the unraveling of the September 11 plot. But, it is at least a possibility that increased analysis, sharing and focus would have drawn greater attention to the growing potential for a major terrorist attack in the United States involving the aviation industry. This could have generated a heightened state of alert regarding such attacks and prompted more aggressive investigation, intelligence gathering and general awareness based on the information our Government did possess prior to September 11, 2001.

Aside from a considerable factual record relating to the September 11th attacks, the hearings before these Committees have also identified systemic problems that have impacted and will, if unresolved, continue to impact the performance of the Intelligence Community. Witnesses have, for example, complained about the lack, prior to September 11th, of sufficient resources to handle far too many broad requirements for intelligence, of which counterterrorism was only one. While requirements grew, priorities were often not updated. As we reported last week, to much of the Intelligence Community, everything was a priority – the U.S. wanted to know everything about everything all the time.

A lack of counterterrorism resources has been a repeated theme through the course of these hearings, particularly in the testimony of witnesses from the Intelligence Community. There has also been some debate about the exact number of analysts at the FBI and the CIA that were dedicated to Bin Ladin and al Q'aida after the DCI's declaration of war on Bin Ladin in December 1998. The CIA has disagreed with the numbers previously reported by the Staff for fulltime UBL analysts within the DCI's Counterterrorism Center (CTC). The Staff was originally given those numbers in interviews with representatives of the CTC. Recently, we have received additional figures on this point from the CIA indicating that, as of August 2001, there were a total of 48.8 FTEs, or the equivalent of about 49 analysts, focused on UBL throughout the entire CIA.

Regarding their resource issues, the FBI has emphasized that FBI headquarters had a number of operations analysts in addition to the one strategic analyst which we had been told of originally by FBI officials and which was noted in our previous staff statement. Our statement, which also noted that some of the FBI's strategic analytic capability on al-Q'aida had been transferred to "operational units", does not dispute that

point. Our focus had been on the FBI's ability to perform strategic, as opposed to operational, analysis of al-Q'aida.

Beyond those specific points, however, I believe that the Staff, the CIA and the FBI are all in agreement that the resources devoted full time to al-Q'aida analysis prior to September 11th paled by comparison to the levels dedicated to that effort after the attacks. As a CIA officer testified during the September 20th Joint Inquiry hearing, both CIA and FBI personnel working on Bin Ladin were "simply overwhelmed" by the workload, prior to September 11th.

Resource issues were not, however, the only systemic problems facing the Intelligence Community. Even aside from the case of al-Mihdhar and al-Hazmi, a number of witnesses described their own experiences with various legal, institutional, and cultural barriers that apparently impeded the Intelligence Community's ability to enhance the value of intelligence through effective and timely information sharing. This is critically important at several levels: within the Intelligence Community itself, between intelligence agencies and other components of the federal government; and between all those agencies and appropriate state and local authorities. Finally, the loss in potential intelligence from a lack of information sharing cuts both ways: we heard from representatives of state and local authorities that, when confronting the threat of terrorist activity within the United States, intelligence obtained at the local level can be critically important.

In the course of these hearings, we also learned of issues that transcend the Intelligence Community and involve questions of policy. In the aftermath of the Cold War, U.S. counterterrorist efforts confronted the emergence of a new breed of terrorists practicing a new form of terrorism, different from the state-sponsored, limited casualty terrorism of the 1960s, 1970s, and 1980s. U.S. counterterrorist efforts faced a host of new challenges, including the rise of Bin Ladin and al-Qa'ida and the existence of a sanctuary in Afghanistan that enabled al-Qa'ida to organize, train, proselytize, recruit, raise funds and grow into a worldwide menace. As Bin Ladin and his "army" flourished within this sanctuary, the United States continued to rely on what was primarily a law enforcement approach to terrorism. As a result, while prosecutions succeeded in taking individual terrorists off the streets, the masterminds of past and future attacks often remained beyond the reach of justice.

Finally, the record suggests that, prior to September 11th, the U.S. intelligence and law enforcement communities were fighting a war against terrorism largely without the benefit of what some would call their most potent weapon in that effort: an alert and committed American public. One need look no further for proof of the latter point than the heroics of the passengers on Flight 93 or the quick action of the flight attendant who identified shoe bomber Richard Reid. While senior levels of the Intelligence Community as well as senior policymakers were made aware of the danger posed by Bin Ladin, there is little indication of any sustained national effort to mobilize public awareness of the gravity and immediacy of the threat prior to September 11th. In the absence of such an effort, there was apparently insufficient public focus on the information that was

available on Bin Ladin, his fatwah against the United States, and the attacks that he had already generated against U.S. interests overseas. As Kristen Breitweiser suggested in her testimony during the first public hearing, could "the devastation of September 11th been diminished in any degree" had the public been more aware, and thus more alert, regarding the threats we were facing during the summer of 2001?

Key Questions for the Committees to Consider

In sum, the record now before these Committees raises significant questions for consideration by policymakers in both Congress and the Executive branch, as they chart the future path of the Intelligence Community in the war against terrorism. For purposes of this public hearing, these include:

- Does the Director of Central Intelligence (DCI) have the power and authority necessary to marshal resources, to instill priorities and to command a consistent response to those priorities throughout the Intelligence Community? When the DCI identified the existence of a "war" against Bin Ladin in 1998, what prevented full mobilization on a war footing throughout the Intelligence Community? What, if any, structural changes are needed to insure greater responsiveness to established priorities and improved collaboration on counterterrorist efforts throughout all parts of the Community?;

- What can be done to significantly improve the quality and timeliness of analytical products throughout the Intelligence Community? Do we have the resources, the training, the skills, the creativity, and the incentives in place to produce excellence in analysis, at both the strategic and tactical levels? Are analysts now focused not only on individual events, but also on the collective significance of the bigger picture? Do we need to create a kind of all-source "fusion center" to maximize our ability to "connect the dots" in the future?;

- What can be done to insure that the Intelligence Community makes the full and best use of the range of techniques available to disrupt, preempt, and prevent terrorist operations? For example, can we improve and increase our use of human intelligence, signals intelligence, liaison relationships with foreign intelligence and law enforcement services, renditions of terrorists abroad for prosecution in U.S. courts, and covert action? Do our intelligence personnel have the training, resources, tools, and incentives needed to use those techniques effectively?;

- Is the Intelligence Community adequately equipped to address the full range of the terrorist threat, both at home and abroad? Has the Community made the adjustments needed to succeed against global terrorist organizations that now include the domestic United States within their range of targets? Have we

established clear channels to facilitate enhanced communication and collaboration between our foreign and domestic intelligence capabilities?;

- Can the FBI effectively shoulder the responsibility of addressing the threat within the United States, including the analysis, collection and sharing of intelligence? Is the traditional law enforcement focus on individual prosecutions compatible with a broader, more proactive focus on intelligence and prevention? If so, what can we do to strengthen the FBI's ability to meet the challenge? If not, where should responsibility for addressing the domestic threat lie?;

- Can the Intelligence Community requirements process be revamped to reflect more accurately legitimate priorities, to simplify the tasks facing collectors and analysts, and to establish a clearer and more credible basis for the allocation of resources? How can we insure that both Intelligence Community requirements and resources keep pace with future changes in the terrorist threat?;

- Do our counterterrorist efforts have full access to the best available information? How can we maximize information sharing within the Intelligence Community, both between agencies and between field operations, management, and other components of individual agencies? In the aftermath of September 11th, can our counterterrorist efforts rely on full access to all relevant foreign and domestic intelligence? Have we finally overcome the "walls" that legal, institutional, and cultural factors had erected between our law enforcement and intelligence agencies?;

- How do we bridge the informational gap that often exists between the Intelligence Community and other federal, state, and local agencies? What can be done to improve the timely dissemination of relevant intelligence to customer agencies? How do we insure that analytic and collection efforts fully benefit not only from information held within the Community, but also from the great wealth of information that exists in other government agencies, as well as the private sector?;

- Can we better harness the benefits of technology to strengthen U.S. intelligence and counterterrorist efforts? When will the FBI be ready to implement technological solutions that will end its longstanding database problems? What, if anything, can be done to speed up that process? Is the Intelligence Community on course to fully utilize data mining and other techniques to greatly improve its collection and analytic capabilities? How can we insure that the Community makes the most of future advances in technology as they occur?;

- Should the Intelligence Community play a greater role in focusing policymakers not only on intelligence but also on those areas where the intelligence suggests defensive or other action may be called for? How can we better insure that future efforts to "harden the homeland" – in areas such as tightening border controls and strengthening civil aviation security – will be identified and implemented before, and not merely after, attacks of the magnitude of September 11th?; and, finally,

- How can we insure that the American public understands and appreciates the full significance and severity of whatever threats may confront this country in the years ahead? How do we balance legitimate national security concerns about the release of intelligence information with the need for the American public to remain alert and committed in efforts as critical as the war against terrorism? How do we maintain, over the long run, a threat warning system that remains both responsible and credible in the eyes of the American public? How can our government, and the Intelligence Community, best explain to the American people not only what happened on September 11th but also what they can expect to face in the future?

Conclusion

Those are, in our view, legitimate and relevant questions, based on the factual record of this Inquiry. The extent to which effective responses are developed and ultimately implemented could significantly impact the future course of counterterrorist efforts, both within and beyond the boundaries of the Intelligence Community. With that in mind and with a view towards the future, we have asked the witnesses today to address the following:

- If the Intelligence Community could replay the years and months prior to September 11, 2001, would the Community do anything differently the second time around?

- What lessons has the Intelligence Community drawn from the September 11 experience?

- What will the Intelligence Community do, in specific terms, to improve future performance?

Mr. Chairmen, that concludes my statement for today.

TESTIMONY OF ELEANOR HILL, STAFF DIRECTOR FOR JOINT INQUIRY

Ms. HILL. Thank you, Mr. Chairman. Chairman Goss, Chairman Graham, members of this Joint Inquiry, good morning.

Over the course of the last few months, these committees have considered a great deal of information, obtained both through witness testimony and through extensive documentary review.

This morning's testimony by the senior leadership of the Intelligence Community will bring to a close this series of open hearings. What has been perhaps unprecedented, at least in terms of the intelligence committees, is the extent to which a good portion of this review has been accomplished through open public hearings. That effort was driven by both the magnitude of September 11 and your recognition of the American public's need to better understand the performance of their government and particularly the Intelligence Community with respect to the events of that day.

Beyond the events of September 11, however, we believe these open hearings have also served to educate the public on the ongoing policy debate about the future path of the Intelligence Community. The considerable factual record that is now before these committees touches on a wide range of issues that are critical to that debate. Ultimately, many of those issues will be considered and will be addressed in even greater depth as these committees deliberate on what will become the final report of this joint inquiry.

At this point, however, the staff has been asked to briefly review the most important elements of the factual record, as well as key questions that we believe have been raised through the course of these public hearings.

Beginning with the initial public hearing, the record describes in considerable detail the situation confronting the U.S. intelligence Community with respect to the terrorist threat posed by Usama bin Ladin prior to September 11. Key facts include: Usama bin Ladin's public fatwa in 1998 authorizing terrorist attacks against American civilians and against military personnel worldwide, U.S. military personnel; information acquired by the Intelligence Community over a 3-year period indicating in broad terms that bin Ladin's network intended to carry out attacks within the United States; the Director of Central Intelligence's statement in December, 1998, that, quote, we are at war, close quote, with bin Ladin and that no resources should be spared by the Intelligence Community in that regard; information accumulated by the Community over the course of a 7-year period indicating that international terrorists had in fact considered using airplanes as weapons; and numerous indicators of a major impending terrorist attack detected by the Community in the spring and summer of 2001.

Although those indicators lack the specifics of precisely where, when or how the attack would occur, the Community had information indicating that the attack was likely to have dramatic consequences for governments and cause mass casualties.

While the specifics of the September 11 attacks were not known in advance, relevant information was available in the summer of 2001. The collective significance of that information was not, however, recognized. Perhaps as a result, the information was not fully

shared in a timely and effective manner, both within the Intelligence Community and with other Federal agencies.

Examples include: In January, 2000, the Central Intelligence Agency succeeded in determining that bin Ladin operatives Khalid al-Mihdhar and al-Hazmi were in Malaysia and in obtaining important information about them. While some information regarding the two was provided to the FBI at an early point, the weight of the evidence suggests that the CIA apparently did not transmit information regarding al-Mihdhar's possession of a U.S. multiple entry visa and the likelihood of travel by the two to the United States, despite various opportunities to transmit all or part of that information in January, 2000; March, 2000; and June, 2001.

On that point, Mr. Chairman, I do want to note—I note in Mr. Tenet's statement for the record this morning he refers to the—there is a January, 2000, CIA message indicating that that information was passed to the FBI. I just want to make clear for the record that we are fully aware of that message. We have referenced it in our previous staff statement.

But we are also aware of the fact that there is considerable other evidence—or I should say lack of evidence on this point to the effect that the information was not passed, which is—my recollection includes interviews of the author of the message who cannot remember the information being passed, interviews of other CIA and FBI individuals who also have no recollection of it being passed, and contemporaneous e-mails, both within the CIA and the FBI, that indicate, while briefings of other issues were provided to the FBI regarding those individuals, that there was no mention of the visa or the information about the possible travel to the U.S.

So my statement is based not simply on the one message but on the weight of all that evidence taken as a whole.

Going on, it was not until late August, 2001, that the CIA watchlisted al-Mihdhar and al-Hazmi and advised the FBI of their likely presence in the United States. FBI efforts to locate them through the New York and Los Angeles FBI offices proved unsuccessful. Other potentially useful Federal agencies were apparently not fully enlisted in that effort. Representatives of the State Department, the FAA and the INS all testified in hearings of this joint inquiry that, prior to September 11, their agencies were not asked to utilize their own information databases as part of the effort to find al-Mihdhar and al-Hazmi.

An FAA representative, for example, testified that he believes that had the FAA been given the names of the two individuals, they would have picked them up in the reservations system.

The FBI did not grasp the significance of a July, 2001, electronic communication from the Phoenix field office identifying a pattern of Middle Eastern males with possible terrorist connections attending flight schools in the United States. Apparently, no one at FBI headquarters connected that idea to previous FBI concerns about the topic or to the increasing threat of a terrorist attack in the summer of 2001.

The communication generated no broader analytic effort on the issue, nor any special alert within the Intelligence Community. Despite its relevance to civil aviation, the FAA did not receive the

communication until it was brought to that Agency's attention in 2002 by the joint inquiry staff.

Also in the summer of 2001, agents in an FBI field office saw in Zacarias Moussaoui a potential terrorist threat, were concerned about the possibility of a larger plot to target airlines and shared those concerns with both FBI headquarters and the DCI's Counterterrorism Center. Neither FBI headquarters nor the CTC apparently connected the information to warnings emanating from the CTC about an impending terrorist attack or to the likely presence of two al-Qa'ida operatives, al-Mihdhar and al-Hazmi, in the United States.

The same unit at FBI headquarters handled the Phoenix electronic communication but still did not sound any alarm bells.

No one will ever know whether more extensive analytic efforts, fuller and more timely information sharing or a greater focus on the connection between these events would have led to the unraveling of the September 11 plot, but it is at least a possibility that increased analysis, sharing and focus would have drawn greater attention to the growing potential for a major terrorist attack in the United States involving the aviation industry. This could have generated a heightened state of alert regarding such attacks and prompted more aggressive investigation, intelligence gathering and general awareness based on the information our government did possess prior to September 11.

Aside from a considerable factual record relating to the September 11 attacks, the hearings before these committees have also identified systemic problems that have impacted and will, if unresolved, continue to impact the performance of the Intelligence Community.

Witnesses have, for example, complained about the lack prior to September 11 of sufficient resources to handle far too many broad requirements for intelligence, of which counterterrorism was only one. While requirements grew, priorities were often not updated. As we reported last week, to much of the Intelligence Community, everything was a priority. The U.S. wanted to know everything about everything all the time.

A lack of counterterrorism resources has been a repeated theme through the course of these hearings, particularly in the testimony of witnesses from the Intelligence Community. There has also been some debate about the exact number of analysts at the FBI and the CIA that are dedicated to bin Ladin and al-Qa'ida after—that were dedicated to bin Ladin and al-Qa'ida after the DCI's declaration of war on bin Ladin in December, 1998. The CIA has disagreed with the numbers previously reported by the staff for full-time UBL analysts within the DCI's Counterterrorism Center.

The staff was originally given those numbers in interviews with representatives of the CTC. Recently, we have received additional figures on this point from the CIA indicating that, as of August, 2001, there were a total of 48.8 FTEs, or the equivalent of about 49 analysts, focused on bin Ladin throughout the entire CIA.

Regarding their resource issues, the FBI has emphasized that FBI headquarters had a number of operations analysts in addition to the one strategic analyst which we had been told of originally by FBI officials and which was noted in our previous staff state-

ment. Our statement, which also noted that some of the FBI's strategic analytical capability on al-Qa'ida had been transferred to, quote, operational units, does not dispute that point. Our focus had been on the FBI's ability to perform strategic as opposed to operational analysis of al-Qa'ida.

Beyond those specific points, however, I do believe that the staff, the CIA and the FBI are all in agreement that the resources devoted full time to al-Qa'ida analysis prior to September 11 paled by comparison to the levels dedicated to that effort after the attacks.

As a CIA officer testified during the September 20th joint inquiry hearing, both CIA and FBI personnel working on bin Ladin were, quote, simply overwhelmed, close quote, by the workload prior to September 11.

Resource issues were not, however, the only systemic problems facing the Intelligence Community. Even aside from the case of al-Mihdhar and al-Hazmi, a number of witnesses have described their own experiences with various legal institutional and cultural barriers that apparently impeded the Community's ability to enhance the value of intelligence through effective and timely information sharing.

This is critically important at several levels, within the Intelligence Community itself, between intelligence agencies and other components of the Federal Government, and between all those agencies and the appropriate State and local authorities.

Finally, the loss in potential intelligence from a lack of information sharing cuts both ways. We heard from representatives of State and local authorities that when confronting the threat of terrorist activity within the United States intelligence obtained at the local level can be critically important.

In the course of these hearings, we also learned of issues that transcend the Community and involve questions of policy. In the aftermath of the Cold War, U.S. counterterrorist efforts confronted the emergence of a new breed of terrorists, practicing a new form of terrorism, different from the state-sponsored, limited casualty terrorism of the 1960s, 1970s and 1980s. U.S. counterterrorist efforts faced a host of new challenges, including the rise of bin Ladin and al-Qa'ida and the existence of a sanctuary in Afghanistan that enabled al-Qa'ida to organize, to train, to proselytize, to recruit, to raise funds and to grow into a worldwide menace.

As bin Ladin and his army flourished within this sanctuary, the United States continued to rely on what was primarily a law enforcement approach to terrorism. As a result, while prosecution succeeded in taking many individual terrorists off the streets, the master minds of past and future attacks often remain beyond the reach of justice.

Finally, the record suggests that, prior to September 11, the U.S. intelligence and law enforcement communities were fighting a war against terrorism largely without the benefit of what some would call their most potent weapon in that effort: an alert and a committed public. One need look no further for proof of the latter point than the heroics of the passengers on flight 93 or the quick action of the flight attendant who identified shoe bomber Richard Reid.

While senior levels of the Intelligence Community as well as senior policymakers were made aware of the danger posed by bin

Ladin, there is little indication of any sustained national effort to mobilize public awareness of the gravity and the immediacy of the threat prior to September 11. In the absence of such an effort, there was apparently insufficient public focus on the information that was available on bin Ladin, his fatwa against the United States and the attacks that he had already generated against U.S. interests overseas.

As Kristen Breitweiser suggested in her testimony during the first public hearing, could, and I quote, the devastation of September 11 been diminished in any degree, close quote, had the public been more aware and thus more alert regarding the threats we were facing during the summer of 2001?

In sum, the record now before these committees raises significant questions for consideration by policymakers in both Congress and the executive branch as they chart the future path of the Intelligence Community in the war against terrorism. For purposes of this public hearing, these include:

Does the Director of Central Intelligence have the power and the authority necessary to marshal resources, to instill priorities and to command a consistent response to those priorities throughout the entire Intelligence Community?

When the DCI identified the existence of a war against bin Ladin, what prevented full mobilization on a war footing throughout the Community?

What, if any, structural changes are needed to ensure greater responsiveness to established priorities and improved collaboration on counterterrorist efforts through all parts of the Community?

What can be done to significantly improve the quality and the timeliness of analytical products throughout the Intelligence Community?

Do we have the resources, the training, the skills, the creativity and the incentives in place to produce excellence in analysis at both the strategic and the tactical levels?

Our analysts now focus not only on individual events but also on the collective significance of the bigger picture. Do we need to create a kind of all-source fusion center to maximize our ability to connect the dots in the future?

What can be done to ensure that the Community makes the full and the best use of the range of techniques available to disrupt, preempt and prevent terrorist operations? For example, can we improve and increase our use of human intelligence, signals intelligence, liaison relationships with foreign intelligence and law enforcement services, renditions of terrorists abroad for prosecution in U.S. courts and covert action?

Do our intelligence personnel have the training, the resources, the tools and the incentives needed to use those techniques effectively?

Is the Community adequately equipped to address the full range of the terrorist threat, both at home and abroad?

Has the Community made the adjustments needed to succeed against global terrorist organizations that now include the domestic United States within their range of targets?

Have we established clear channels to facilitate enhanced communication and collaboration between our foreign and domestic intelligence capabilities?

Can the FBI effectively shoulder the responsibility of addressing the threat within the United States, including analysis, collection and sharing of intelligence?

Is the traditional law enforcement focus on individual prosecutions compatible with the broader, more proactive focus on intelligence and prevention? If so, what can we do to strengthen the FBI's ability to meet that challenge? If not, where should responsibility for addressing the domestic threat lie?

Can the Intelligence Community requirements process be revamped to reflect more accurately legitimate priorities to simplify the tasks facing collectors and analysts and to establish a clearer and more credible basis for the allocation of resources?

How can we ensure that both the Community requirements and resources keep pace with future changes in the terrorist threat?

Do our counterterrorist efforts have full access to the best available information?

How can we maximize information sharing within the Community, both between agencies and between field operations, management and other components of individual agencies?

In the aftermath of September 11, can our counterterrorist efforts rely on full access to all relevant foreign and domestic intelligence?

Have we finally overcome the walls that legal, institutional and cultural factors had erected between our law enforcement and intelligence agencies?

How do we bridge the informational gap that often exists between the Community and other Federal, State and local agencies?

What can be done to improve the timely dissemination of relevant intelligence to customer agencies?

How do we ensure that analytic and collection efforts fully benefit not only from information held within the Community but also from the great wealth of information that already exists in other government agencies as well as the private sector?

Can we better harness the benefits of technology to strengthen U.S. intelligence and counterterrorist efforts?

When will the FBI be ready to implement technological solutions that will end its long-standing database problems? What, if anything, can be done to speed up that process?

Is the Intelligence Community on course to fully utilize data mining and other techniques to greatly improve its collection and analytic capabilities?

How can we ensure that the Community makes the most of future advances in technology as they occur?

Should the Intelligence Community play a greater role in focusing policymakers not only on intelligence but also on those areas where the intelligence suggests defensive or other action may be called for?

How can we better ensure that future efforts to harden the homeland in areas such as tightening border controls and strengthening civil aviation security will be identified and will be imple-

mented before and not merely after attacks of the magnitude of September 11?

And, finally, how can we ensure that the American public understands and fully appreciates the significance and the severity of whatever threats may confront this country in the years ahead?

How do we balance legitimate national security concerns about the release of intelligence information with the need for the American public to remain alert and committed in efforts as critical as the war against terrorism?

How do we maintain over the long run a threat warning system that remains both responsible and credible in the eyes of the American people?

How can our government and the Intelligence Community best explain to the American people not only what happened on September 11 but also what they can expect to face in the future?

Those are, in our view, legitimate and relevant questions based on the factual record of this inquiry. The extent to which effective responses are developed and ultimately implemented could significantly impact the future course of counterterrorist efforts, both within and beyond the boundaries of the Intelligence Community.

With that in mind and with a view towards the future, we have asked the witnesses today to address the following:

First, if the Intelligence Community could replay the years and months prior to September 11, 2001, would the Community do anything differently the second time around?

Second, what lessons has the Community drawn from the September 11 experience?

And, third, what will the Intelligence Community do in specific terms to improve future performance?

Mr. Chairman, that concludes my statement.

Chairman GRAHAM. Ms. Hill, thank you for another outstanding presentation which has brought a high level of insight and analysis to complex questions. Your service and your colleagues on our joint inquiry staff have performed a great national service for which we are deeply in debt.

Ms. HILL. Thank you, Mr. Chairman.

Chairman GRAHAM. Before introducing Directors Tenet and Mueller and General Hayden, at our request the heads of two other important components of our Intelligence Community have submitted statements for the record.

The statements are from Lieutenant General James Clapper, United States Air Force Retired, the Director of the National Imagery and Mapping Agency, and Rear Admiral Joel Jacoby, the acting director of the Defense Intelligence Agency.

I ask unanimous consent that their statements be made part of the record. Is there objection? Without objection, so ordered.

[The prepared statements for the record of Lieutenant General Clapper and Rear Admiral Jacoby follow:]

Statement for the Record

Submitted by

Lieutenant General James R. Clapper Jr, USAF, Ret.

Director

National Imagery and Mapping Agency

Before the

Joint Inquiry of

Senate Select Committee on Intelligence

And

House Permanent Select Committee on Intelligence

Performance of the Intelligence Community
Concerning September 11, 2001

17 October 2002

Chairmen, members of the committees, I welcome the opportunity to report on the National Imagery and Mapping Agency's (NIMA) efforts to improve the collection and sharing of terrorism related information.

NIMA's mission of providing timely, relevant, and accurate Geospatial Intelligence in support of national security objectives is more vital than ever in protecting America's interests. It is with great pride that I can report to this joint committee on the outstanding efforts and accomplishments of the men and women of NIMA in support of the Global War on Terrorism. On the other hand, we also face continuing challenges, and I will outline how NIMA is now postured to tailor our Geospatial Intelligence support in the future.

While the attacks of 9/11 profoundly changed our perception of what we now soberly understand as "national security," the counterterrorism mission was not a new one to NIMA. Since long before our stand-up in 1996, NIMA's predecessor organizations were involved in the Intelligence Community's approach to locate, identify and analyze global terrorism-related activity. NIMA has capitalized on these efforts and now converges the traditional categories of imagery, imagery intelligence, and geospatial data and information, into what we now refer to as Geospatial Intelligence. Geospatial Intelligence, which forms the foundational baseline for all subsequent analysis,

encompasses all the skills, expertise, and capabilities that reside in NIMA today and signals our new vision: *"Know the Earth... Show the Way."*

NIMA, as the National Geospatial Intelligence functional manager, is responsible both to the Director of Central Intelligence (DCI) and to the Secretary of Defense (SecDef) to ensure vast imagery and geospatial resources are effectively applied across the various organizations in which they reside. To that end, NIMA must "show the way" in the sense of promoting interoperability and standardization, and across the realms of tasking, collection, processing, exploitation, and dissemination. The terrorism threat has crystallized the imperative for what we term the "ubiquitous knowledge map" – and NIMA is assuming responsibilities for its Geospatial Intelligence standards, structure, and content.

Geospatial Intelligence is a critical contributor to the counterterrorism mission. First, it provides a common reference of where things are on the earth, and augments the temporal all-source analysis of terrorists' activities. When combined with human intelligence (HUMINT) and/or signals intelligence (SIGINT), Geospatial Intelligence helps to identify and monitor terrorist activity. However, it cannot determine intent. Geospatial Intelligence is also crucial for planning and executing operations. In sum, we enable national and military decision makers to understand and see the strategic terrorism intelligence picture. However, Geospatial Intelligence cannot provide the entire picture; it cannot be a primary source of tactical information. It has been of greatest use for strategic description of long-term trends.

Before September 11, 2001, NIMA's counterterrorism analytical effort focused on supporting requirements of the DCI and the SecDef. Whether we were executing our global mission to provide a geospatial foundation for further analysis, or supporting specific requirements of our partners, NIMA's small but expert analytical cadre met the Geospatial Intelligence needs of the Intelligence Community. Well before September 11, we had worked closely with the CIA and the Joint Staff in support of operational planning and its execution. Since September 11, we have intensified this work by establishing our own Office of Counter Terrorism, and by bolstering our on-site support to the CIA and the military's Joint Intelligence Task Force for Combating Terrorism (JITF-CT).

Geospatial Intelligence, cued by other sources, provides the analytical foundation for understanding the overall terrorism picture. For example, working in a collaborative intelligence source mode, we have located and identified numerous terrorist sites. Correspondingly, other disciplines have leveraged Geospatial Intelligence to refine their own collection and analysis. To further improve this initiative as well as our own collaboration with another agency, we now have NIMA analysts performing hands-on integration of our two disciplines and providing Geospatial Intelligence, as needed.

Throughout our history of support to the counterterrorism mission, NIMA has ensured timely, relevant, and accessible reporting to our national and DoD customers. Early on, NIMA recognized the interdependent nature of Geospatial Intelligence and its

partnership role with the other established intelligence disciplines. From participating in daily briefings with senior Intelligence Community leaders; chairing collection requirements activities; collocating our analysts within our customers' facilities; to providing our customers on-line, worldwide access to our digital Geospatial Intelligence, NIMA continues to improve our ability to reach out and connect at all levels with our customers. As we work with our intelligence partners, we fully understand that the sum is truly greater than the parts.

In the wake of September 11, NIMA streamlined to better meet the threat and put the agency on a war footing. We have since begun to significantly transform NIMA to modernize our infrastructure, which will enable refocused analysts to collaborate better among themselves and with the community. Much of this is tied to doing better against the counterterroism problem. NIMA's success is dependent on:

- Clear priorities and customer support to allow us to efficiently prioritize our activities.
- Multi-intelligence source collaboration and analysis gives us the best available cueing, directs our research, and allows us to make the most informed judgments-- for we recognize that even at its most robust, Geospatial Intelligence alone cannot work against the terrorism issue. Flexibility and depth allows us to surge significant numbers of Geospatial Intelligence analysts to support terrorism and other crises worldwide. This capability relies on having a cadre of trained, experienced, and motivated analysts.

- The right technology and systems to collect against moving targets or underground targets and the ability to integrate all sources of imagery into the National System for Geospatial Intelligence (NSGI) architecture, with round-the-clock availability. This is an end-to-end capability improvement; more or better types of collection are meaningless if we don't also have the systems to use and move information.

A major driver for our transformation is to expand our ability to conduct surveillance, as opposed to reconnaissance. The latter, which has been our traditional method of operation, does not allow for the intense scrutiny of subtle signs that are necessary to address the terrorism target. We increasingly are engaging in surveillance work. Additionally, we are increasing the utility of reconnaissance by expanding the use of the full range of capabilities in the imagery spectrum.

NIMA will cooperate closely with other agencies as they devise a tactical/strategic warning system. We have longstanding experience in this kind of activity, as demonstrated in our work with organizations such as the Federal Emergency Management Agency, with whom we are able to pass critical information rapidly, across the nation, and at multiple levels of government. Fundamentally, for NIMA it does not matter which agency would be the lead for constructing and operating a warning program; we have the systems and experienced personnel needed to be an effective contributor, regardless of where the program is centered.

We are expanding our work with liaison services, and receive their reporting as it is published. We in turn make their analysis available to the larger US Intelligence Community. NIMA has been expanding its outreach to the Intelligence Community and will continue to do so. We have close and continuing contact with the Office of Homeland Security, and participate with intelligence and law enforcement agencies in actions such as securing the Olympics and other events. We currently contribute officers to staff the Joint Intelligence Task Force for Combating Terrorism. We have established full-time liaison at the FBI, continue our longstanding and very close collaboration with the CIA, and are doubling our presence at NSA. We believe that these measures will greatly enhance the application of Geospatial Intelligence across the Community and encourage better analytic interchange.

NIMA's structure and emphasis are in consonance with the DCI's guidance on intelligence priorities. We have already moved significant resources to the counterterrorism mission in our Office of Counter Terrorism. Moreover, we have accelerated the rate of planned growth for that office, so that it will meet its projected end strength sooner than originally planned. In addition, we have established a North America Homeland Security Division in our Office of the Americas. NIMA has increased almost tenfold the number of analysts dedicated to the counterterrorism and Homeland Security missions. These and other adjustments to meet DCI priorities have come entirely from within internal personnel resources.

While we remain careful with sensitive signatures, one of the virtues of Geospatial Intelligence is that it usually can be disseminated widely, at relatively low levels of classification. Also, it is often very literal in that it can present information using imagery on a geospatial background, that is to say a picture that also shows terrain perspectives or "lay of the land". This makes it useful to many analysts and consumers and fosters collaboration and rapid use by first responders, as the geospatial common denominator.

As with the rest of the Community, NIMA faces demanding challenges just from the volume of information that comes to us every day. NIMA is reordering investment priorities to allow us to strengthen our infrastructure across the board. At the same time, we are exploring technologies to enable smarter handling of the raw data that come to us. An additional concern is the need to grow expertise as we expand the size of our organizations working counterterrorism. Most of our analysts are either quite junior, with only a few years of service, or are new to counterterrorism. Strengthening this capability will be challenging for the agency over the next several years.

Chairmen, members of the Committees, the National Imagery and Mapping Agency continues to do everything in our power to identify those responsible for past attacks, to detect and identify current terrorist-related activity to get this information to policy makers, military commanders, and homeland defenders with a view to prevent future terrorist attacks. In support of our community partners and customers, NIMA is dedicated to winning this Global War on Terrorism by shedding light on their locations, discovering their activities, and supporting their eradication. As I said at the outset, we

are very proud of our record of analytical support and community collaboration and we look forward to continuing our contributions to winning the Global War on Terrorism-- at home and abroad.

STATEMENT FOR THE RECORD

FOR

THE JOINT 9/11 INQUIRY

10 October 2002

DIA RESPONSE TO JOINT 9/11 LETTER OF INVITATION

Rear Admiral Lowell E. Jacoby, US Navy
Acting Director, Defense Intelligence Agency

Statement for Record
Rear Admiral Lowell E. Jacoby, United States Navy
Acting Director, Defense Intelligence Agency
10 October 2002

Chairman Graham, Chairman Goss, members of these Committees, thank you for another opportunity to address the performance of the Intelligence Community concerning the September 11, 2001 terrorist attacks against the United States. I appreciate your Committees' focus on identifying actions that will strengthen the Intelligence Community, enabling us to better detect and prevent future terrorist attacks.

Rather than repeat the detailed responses from our earlier statements, I want to focus on five lessons-learned concerning the terrorism threat to the United States. In exploring these lessons, I will cover the three general questions posed in your letter – what we could have done differently, what we derived from the experience, and what we are doing about it – as well as the range of specific subjects you requested I address.

The first and earliest lesson-learned is that we must largely reject previously held assumptions about the magnitude and nature of the terrorist threat to the United States. Similarly, we must constantly and methodically reassess current assumptions about terrorists' operational behavior and decision-making.

Next, as a community, we must work as a unified body to focus on the threat and not allow organizational, jurisdictional, or territorial boundaries to diminish the effectiveness of our efforts. We must close any intra-governmental seams that can be exploited by an adaptive, transnational, and elusive adversary.

Third, we must reengineer the community's information management paradigm. Information is the raw material of the intelligence business and we must find ways to extract additional value from what is currently available while at the same time harvesting and exploiting new and non-traditional sources of data.

Fourth, we can take little comfort in strategic warning where the threat of terrorism is concerned. The nature of the threat demands warning with tactical perspective, timeliness, and specificity. A natural tendency to "over-warn" must be recognized and overcome.

And finally, the war on terrorism is a long-term proposition that demands extraordinary continuity of purpose, focus, and resource commitment. We cannot allow a lull in terrorist attacks – no matter how long it might extend – to engender a false sense of security and a lowering of priority.

Prior to the 11 September attacks, terrorist operations against United States' interests were not seen as posing a grave threat to the national security of the United States. I am not downplaying the gravity of these attacks, as they had serious and tragic impact on our activities, people, and interests overseas. However, the 11 September strikes at the core of America's military, political, and economic systems changed forever the way we view the terrorist threat.

We were surprised analytically by the complexity of the overall plan, the stunning simplicity of "weaponizing" for mass casualties, and the benign backgrounds of the individual attackers. Our underlying assumptions about bin Ladin's creativity and limits on his actions were wrong. In short, long-held analytic assumptions about terrorist groups and their intentions, values, constraints, and methods of operation – which were challenged by the earlier attack on the USS COLE -- were completely shattered on 11 September.

Maintaining a government-wide, carefully orchestrated counterterrorism effort is critical. Terrorists not only recognize and respect no geographic boundaries; they are committed to aggressively discerning cracks, or seams, in our defenses. Jurisdictional -- and sometimes "turf" -- lines between foreign intelligence activities and law enforcement

responsibilities, particularly in the domestic context, represents that type of potential seam.

While the hand-off mechanisms between and among intelligence and law enforcement agencies work fairly well, they have to extend further and become more institutionalized. In doing that, we must ensure a steady flow of information, expertise, and insight both horizontally and vertically – that is, from National to State to Local, and the reverse. I recognize and accept that some information cannot be fully shared. But, what can be shared must be shared.

Our measures of success must lie in the area of effectiveness, not efficiency. While some issues are prime candidates for cross-community economizing – i.e. distributed or federated analysis, product deconfliction, strict division of labor– terrorism is not one of them. Some of the potential seams in our defenses may best be closed by overlapping efforts and responsibilities. Terrorism is an issue where competitive analysis is essential; planned duplication and redundancy by design are virtues.

The benefit of competitive analysis is optimized only when all parties have access to the same information base. The act of drawing different – even opposing – conclusions from a common body of evidence should be encouraged. It is an opportunity to extract additional "meaning" from fragmentary data, ultimately increasing the precision and impact of our collective threat analyses. I remain steadfast in my belief – elaborated upon in previous statements -- that the analytic component of the Intelligence Community can make a greater contribution to the war on terrorism if given access to a much wider range of information and supported with more capable technologic tools.

One part of gaining wider access to potentially relevant information is technology-based; the others are cultural or procedural. On the technology front, we are moving our Joint Intelligence Task Force for Combating Terrorism (JITF-CT) into a completely transformed information management environment based on best practices and standards of the commercial sector. By transitioning to eXtensible Markup

Language (XML) standards and initiating data-tagging at the content level, we can begin reaping the substantial benefits of modern data mining and "analytic discovery" tools. Our ultimate objective is to achieve interoperability at the data level, rather than the system level.

In short, we know we can improve the power and performance of existing information and, at the same time, prepare to assimilate and exploit new sources and types of information to which we are seeking greater access. Since 11 September, the JITF-CT has achieved much greater access to some types of information and progress is being made on others. We are committed to incorporating a wider range of previously under-tapped law enforcement/security information into JITF-CT's analyses and see no insurmountable obstacles to doing so. Of note, doing so requires re-defining the traditional view of intelligence collection when it comes to terrorism.

In discerning terrorist intentions and to provide tactical warning, it is desperately important that we harvest and exploit more information on terrorists' pre-incident behavior and activity. There are scores – in some cases hundreds – of discrete steps taken by terrorists as they choose, plan, and move in on a target. For the most part, each step, when observed in isolation, may appear to be everyday, routine activity. For example, the purchase or forgery of travel documents, "accidental" intrusions in secure areas, or movement of cash may have innocent explanations and benign implications. But maybe not.

During the pre-incident period, potential indications of terrorist activities are far more likely to be observed by police, security, or bystanders than by traditional intelligence collectors. We need to do a much better job of incorporating this type of information into our analytic equation. While ninety-nine percent of it will likely turn out to be "noise," we cannot afford to miss the one percent that is not. Provision of tactical warning is dependent on receiving and understanding tactical-level indicators.

Once analysis of indicators reveals a threat, the next step is, of course, timely dissemination of warning. Much like the collection arena, the indications and warning arena for terrorism poses unique dilemmas for the community. For many issues, we judge the effectiveness of our warning efforts by the accuracy rate of our predictions – i.e. of the events forecasted, how many did, in fact, occur? In predictions, an eighty percent accuracy rate is considered very commendable. Conversely, terrorism warning, when effective, causes action to be taken which prevents the event. A predictive accuracy rate of zero is the desired goal. Prevention, not prediction, is the measure of effectiveness for terrorism warning.

The Defense Intelligence Agency has invested heavily in terrorism warning. Force Protection has been, and will continue to be, among our most important missions. In that regard, the "*Report of the DOD Commission on the Beirut International Airport (BIA) Terrorist Act, 23 October 1983,*" (Long Commission Report), continues to serve as the prevailing benchmark for our terrorism warning efforts. Among the intelligence inadequacies documented in that report was the injudicious issuance of a constant stream of "chicken little" warnings.

Over-warning – particularly the broad dissemination of generalized, non-actionable alerts – unquestionably degrades and ultimately subverts the intent and effect of the warning process. On that note, I should point out that the Intelligence Community's guidelines for issuing terrorist threat alerts and advisories are exactly right. Collectively, we must exercise the discipline to adhere to them.

Discipline may also be required to ensure we sustain the momentum, focus, and resources needed for an extended, war on terrorism. Unfortunately, governmental attention on terrorism has been episodic, rising sharply in the aftermath of major events – such as the downing of Pan Am Flight 103 or the attacks on our embassies, Khobar Towers, and USS COLE – and declining noticeably as the months pass without an additional attack. In some cases, resources that were apportioned to address the threat of terrorism were diverted or diluted as soon as the episodes of high attention subsided.

Since 11 September, the U.S. has employed extraordinary security measures at home and abroad. We have enjoyed unprecedented cooperation on terrorism intelligence and security issues from governments across the globe. Within our own government, we devised new ways to cooperate and collaborate and have allotted very significant resources and energy to the war on terrorism. Great progress has been made. The result of our collective effort is a particularly difficult operating environment for terrorists.

However, as history shows, terrorists work on their own timelines. They are content to wait months or years to increase their chances of success or the lethality of a specific action. In many ways, terrorism is like a cancer that invades an unsuspecting body even as it appears free of outward symptoms. A prolonged lull in terrorist attacks does not infer a diminished threat. In fact, akin to the paradox inherent in terrorism warning – a preventive not predictive process that seeks zero percent predictive accuracy – it is not difficult to argue that the longer we go with out a major attack, the closer we are to the next one. Constancy of purpose, continuity of focus, and unity of effort must be our watchwords. Thank you.

Chairman GRAHAM. In addition, General Clapper and Admiral Jacoby have each designated a representative to be in attendance today in the event that any member of the committee has a question for their agencies.

The representatives are Ms. Jennifer Haley, chief of NIMA's counterterrorism special operations, and Mr. Pat Ducey, head of the Joint Intelligence Tasks Force for Counterterrorism from the DIA.

I would now like to introduce the members of our distinguished panel. Mr. George Tenet was sworn in as Director of the Central Intelligence Agency on July 11, 1997. In that capacity, he has responsibilities relating to the entire United States Intelligence Community as well as directing the Central Intelligence Agency. He previously served as the Deputy Director of the CIA and in a senior position at the National Security Council.

Prior to his executive branch service, Mr. Tenet served for four years as the Staff Director of the Senate Intelligence Committee.

Robert Mueller was sworn in as Director of the Federal Bureau of Investigation on September 4, 2001. He has served in both line and supervisory capacities as a Federal prosecutor, including as United States Attorney for the District of Massachusetts and later the Northern District of California. He has also served as Assistant Attorney General in charge of the Department of Justice's criminal division and, for a period, as Acting Deputy Attorney General of the United States.

Lieutenant General Michael Hayden has been the Director of the National Security Agency since March 1999. His long and distinguished tenure in the Air Force has included service as commander of the Air Intelligence Agency, Director of the Joint Command and Control Warfare Center, and Deputy Chief of Staff, United Nations Command, and U.S. Forces Korea.

Each of our committees has adopted a supplemental rule for this joint inquiry that all witnesses will be sworn. I ask Directors Tenet and Mueller and General Hayden to please rise at this time, along with the NIMA and DIA representatives, Ms. Haley and Mr. Ducey.

[Witnesses sworn.]

Chairman GRAHAM. Thank you. The full statements of the witnesses will be placed in the record of these proceedings. We have a large number of our members present, and I know that they have a significant and incisive series of questions.

Therefore, I am going to ask if our panelists could summarize their statements into approximately ten minutes so that we will maximize the time for questions.

At this time, I will call on Directors Tenet, Mueller and General Hayden, in that order, to give their opening remarks.

Mr. Tenet.

[The prepared statement of Mr. Tenet follows:]

Written Statement for the Record of the
Director of Central Intelligence
Before the
Joint Inquiry Committee
17 October 2002

I welcome the opportunity to be here today and to be part of an inquiry that is vital to all Americans. On September 11th, nearly three thousand innocent lives were taken in brutal acts of terror. For the men and women of American Intelligence, the grief we feel—the grief we share with so many others—is only deepened by the knowledge of how hard we tried—without success—to prevent this attack.

It is important for the American people to understand what CIA and the Intelligence Community were doing to try to prevent the attack that occurred - and to stop attacks, which al-Qa'ida has certainly planned and remains determined to attempt.

What I want to do this morning, as explicitly as I can, is to describe the war we have waged for years against al-Qa'ida -- the level of effort, the planning, the focus, and the enormous courage and discipline shown by our officers throughout the world. It is important for the American people to understand how knowledge of the enemy translated into action around the globe—including the terrorist sanctuary of Afghanistan—*before* September 11.

It is important to put our level of effort into context...to understand the tradeoffs in resources and people, we *had* to make - the choices we consciously made to ensure that we maintained an aggressive counterterrorist effort.

We need to understand that in the field of intelligence, long-term erosions of resources cannot be undone quickly when emergencies arise. And we need to explain the difference that sustained investments in intelligence—particularly in people—will mean for our country's future.

We need to be honest about the fact that our homeland is very difficult to protect. For strategic warning to be effective, there must be a dedicated program to address the vulnerabilities of our free and open society. Successive administrations, commissions, and the Congress have struggled with this.

To me, it is not a question of surrendering liberty for security, but of finding a formula that gives us the security we need to defend the liberty we treasure. Not simply to defend it in time of peace, but to preserve it in time of war—a war in which we must be ready to play offense and defense simultaneously. That is why we must arrive—soon—at a national consensus on Homeland Security.

We need to be honest about our shortcomings, and tell you what we have done to improve our performance in the future. There have been thousands of actions in this war—an intensely human endeavor—not all of which were executed flawlessly. We made mistakes.

Nevertheless, the record will show a keen awareness of the threat, a disciplined focus, and persistent efforts to track, disrupt, apprehend, and ultimately bring to justice Bin Ladin and his lieutenants.

Somehow lost in much of the debate since September 11 is one unassailable fact: The US intelligence community could not have surged, as it has in the conflict in Afghanistan, and engaged in an unprecedented level of operations around the world, if it was as mired as some have portrayed.

It is important for the American people to know that, despite the enormous successes we have had in the past year—indeed over many years—al-Qa'ida continues to plan and will attempt more deadly strikes against us. There will be more battles won and, sadly, more battles lost. We must be honest about that, too.

Finally, we need to focus on the future, and consider how the knowledge we have gained in this war will be applied.

These are some of the themes that I hope you will reflect on as you listen to this testimony today.

Let me begin by describing the rise of Usama Bin Ladin and the Intelligence Community's Response.

- We recognized early on the threat posed by Usama Bin Ladin and his supporters.
- As that threat developed, we tracked it and we reported it to Executive Branch policymakers, Congress, and, when feasible, directly to the American people.
- We reacted to the growing threat by conducting energetic, innovative, and increasingly risky operations to combat it. We went on the *offensive*.
- And this effort *mattered*. It saved lives—perhaps in the thousands. And it prepared the field for the rapid successes in Afghanistan last winter.

The Early Years: Terrorist Financier (1986-1996)

The first rule of warfare is "know your enemy." My statement documents our knowledge and analysis of Bin Ladin, from his early years as a terrorist financier to his leadership of a worldwide network of terrorism based in Afghanistan.

Bin Ladin gained prominence during the Afghan war for his role in financing the recruitment, transportation, and training of Arab nationals who fought alongside the Afghan mujahedin against the Soviets during the 1980s.

- While we knew of him, we have no record of any direct US Government contact with Bin Ladin at that time.

- Bin Ladin came to the attention of the CIA as an emerging terrorist threat during his stay in Sudan from 1991 to 1996.

CIA reported that during Bin Ladin's five-year residence in Sudan he combined business with *jihad* under the umbrella of al-Qa'ida.

- In May 1993, for example, al-Qa'ida financed the travel of more than 300 Afghan war veterans to Sudan after the Pakistani government launched a crackdown against foreign Islamic extremists based in Pakistan.

- By January 1994, al-Qa'ida had begun financing at least three terrorist training camps in northern Sudan. Among the trainers were Egyptian, Algerian, Tunisian, and Palestinian extremists.

- Islamic extremists, who in December 1992 bombed a hotel housing US servicemen in Aden, Yemen, said Bin Ladin financed their group.

- We learned in 1996 that Bin Ladin sent members to Somalia in 1993 to work as advisors with Somali warlord Aideed in opposing US forces sent there in support of Operation Restore Hope. Bin Ladin later publicly claimed responsibility for this activity, and CIA has confirmed his involvement in Somalia.

- After Bin Ladin had left Sudan we learned that al-Qa'ida had attempted to acquire material used in pursuing a chemical, biological, radiological, nuclear (CBRN) capability and had hired a Middle Eastern physicist to work on nuclear and chemical projects in Sudan.

As Bin Ladin's prominence grew in the early 1990's, it became clear to CIA that it was not enough simply to collect and report intelligence about him.

- As early as 1993, our units watching him began to propose action to reduce his organization's capabilities.

I must pause here. In an open forum I cannot describe what authorities we sought or received. But it is important that the American people understand two things.

- The first is about covert action in general: CIA can only pursue such activities with the express authorization of the President.

- The second point is that, when such proposals are considered, it is always because we or policymakers identify a threatening situation, a situation to which we must pay far more attention and one in which we must run far greater risks. As long ago as 1993, we saw such a situation with Usama Bin Ladin.

By the time Bin Ladin left Sudan in 1996 and relocated himself and his terror network to Afghanistan, the Intelligence Community was taking strong action to stop him.

- We established a special unit--known as the Bin Ladin Issue Station--with CIA, NSA, FBI and other officers specifically to get more—and more actionable—intelligence on Bin Ladin and his organization. We took this step because we knew that traditional approaches alone would not be enough for this target.

- We monitored his whereabouts and increased our knowledge about him and his organization with information from our own assets and from many foreign intelligence services.

- We were working hard on an aggressive program to disrupt his finances, degrade his ability to engage in terrorism, and, ultimately, to bring him to justice.

We must remember that, despite this heightened attention, Bin Ladin was in the mid-1990s only one of four areas of concentration within our Counter-Terrorist Center, CTC.

- In addition to the Bin Ladin Issue Station, we had a group working against Hizballah; a group working Egyptian Islamic Jihad, al-Gama'at, and Palestinian rejectionists; and a group working on an assortment of smaller terrorist groups, such as Shining Path in Peru, Abu Sayef in the Philippines, and the Tamil Tigers of Sri Lanka.

Taliban Sanctuary Years: Becoming a Strategic Threat

Beginning in January 1996, we began to receive reports that Bin Ladin planned to move from Sudan. Confirming these reports was especially difficult because of the closure in February of the US Embassy as well as the CIA station in Khartoum for security reasons.

- We have read the allegations that, around this time, the Sudanese Government offered to surrender Bin Ladin to American custody.

- Mr. Chairman, CIA has no knowledge of such an offer.

Later in 1996, it became clear that he had moved to Afghanistan. From that safehaven, he defined himself publicly as a threat to the United States. In a series of declarations, he made clear his hatred for Americans and all we represent.

- In July 1996, Bin Ladin described the killing of Americans in the Khobar Towers bombing in Saudi Arabia in June 1996 as the beginning of a war between Muslims and the United States.

- One month later, in August 1996, Bin Ladin issued a religious edict or *fatwa* entitled *"Declaration of War,"* authorizing attacks against Western military targets on the Arabian Peninsula.

- In February 1998, six months prior to the US Embassy bombings in East Africa, al-Qa'ida—under the banner of the "World Islamic Front for Jihad Against Jews and Crusaders"—issued another *fatwa* stating that all Muslims have a religious duty "to kill Americans and their allies, both civilian and military" worldwide.

By the time of the 1998 East Africa bombings, al-Qa'ida had established its intention to inflict mass casualties and a modus operandi emphasizing careful planning and exhaustive field preparations, which Bin Ladin saw as a prerequisite for the type of spectacular operations he had in mind.

- For example, when asked in a November 1996 interview why his organization had not yet conducted attacks in response to its August *fatwa* statement, Bin Ladin replied, "If we wanted to carry out small operations, it would have been easy to do so after the statements, but the nature of the battle requires qualitative operations that affect the adversary, which obviously requires good preparation."

The East Africa bombings in August 1998 and the attack on the USS Cole in October 2000 succeeded because of al-Qa'ida's meticulous preparation and effective security practices.

- CIA analysts looked at captured al-Qa'ida targeting studies and training materials around the time of the East Africa and USS Cole attacks. They published an in-depth intelligence study of al-Qa'ida's terrorist operations that revealed that much of the terrorists' advance planning involved careful, patient, and meticulous preparation.

Beyond the conventional threat, we were also becoming increasingly concerned—and therefore stepped up our warning—about al-Qa'ida's interest in acquiring unconventional weapons, not only chemical or biological elements, but nuclear materials as well.

- In a December 1998 interview, Bin Ladin called the acquisition of these weapons a "religious duty" and noted, "How we would use them is up to us."

- We reported in 1998 that an extremist associated with Al-Qa'ida said Bin Ladin was seeking a "Hiroshima."

- As early as July 1993, in testimony to the House Foreign Affairs Committee, DCI Woolsey warned of the Intelligence Community's heightened sensitivity to the prospect that a terrorist incident could involve weapons of mass destruction (WMD). In February 1996, in testimony to the Senate Select Committee on Intelligence, DCI Deutch expressed his concern about the growing lethality, sophistication, and wide-ranging nature of the terrorist threat, and that terrorists would push this trend to its most "awful extreme by employing weapons of mass destruction." I made similar warnings to these committees as early as 1998, when I pointed to Bin Ladin's attempts to purchase or manufacture biological and chemical weapons for an attack against US facilities.

- CIA analysts published two in-depth assessments on al-Qa'ida's CBRN capabilities in 1999.

The terrorist plotting, planning, recruiting, and training that Bin Ladin and al-Qa'ida did in the late 1990s were aided immeasurably by the sanctuary the Taliban provided.

- Afghanistan had served as a place of refuge for international terrorists since the 1980s. The Taliban actively aided Bin Ladin by assigning him guards for security, permitting him to build and maintain terrorist camps, and refusing to cooperate with efforts by the international community to extradite him.

- In return, Bin Ladin invested vast amounts of money in Taliban projects and provided hundreds of well-trained fighters to help the Taliban

consolidate and expand their control of the country.

- While we often talk of two trends in terrorism—state-supported and independent—in Bin Ladin's case with the Taliban we had something completely new: a *terrorist* sponsoring a *state*.

Afghanistan provided Bin Ladin a relatively safe operating environment to oversee his organization's worldwide terrorist activities.

- Militants who received training there were sent afterwards to fight in *jihads* in Kashmir, Chechnya, or Bosnia.

- The al-Qa'ida/Taliban training camps formed the foundation of a worldwide network by sponsoring and encouraging Islamic extremists from diverse locations to forge longstanding ideological, logistical, and personal ties.

- Extremists in the larger camps received basic training in the use of small arms and guerrilla tactics. In the smaller camps, militants received more advanced and specialized training in subjects like explosives, poisons, and assassination techniques.

- Clandestine and counterintelligence tradecraft courses included basic instruction on how to establish secure, cell-based, clandestine organizations to support insurgencies or terrorist operations.

- Indoctrination in extremist religious ideas was emphasized and included the repetition of ideas that the United States is evil, and that the regimes of Arab countries are not true believers in Islam and should be overthrown as a religious duty.

- Some of the Afghan camps provided the militants instruction in the production and use of toxic chemicals and biological toxins.

In summary, what Bin Ladin created in Afghanistan after he relocated there in 1996 was a sophisticated adversary—as good as any that CIA has ever operated against.

Going to War against al-Qa'ida—"The Plan"

As the Intelligence Community improved its understanding of the threat, and as the threat grew, we refocused and intensified our efforts to track, disrupt, and bring the terrorists to justice.

By 1998, the key elements of the CIA's strategy against Bin Ladin and al-Qa'ida—inside Afghanistan and globally—placed us in a strongly offensive posture. They included:

- Hitting al-Qa'ida's infrastructure;
- Working with foreign security services to carry out arrests;
- Disrupting and weakening UBL's businesses and finances;
- Recruiting or exposing operatives; and
- Pursuing a multi-track approach to bring Bin Ladin himself to justice, including working with foreign services, developing a close relationship with US federal prosecutors, increasing pressure on the Taliban, and enhancing our capability to capture him.

CIA's policy-and-objectives statement for the FY 1998 budget submission to Congress—which was prepared in early 1997—reflects this determination to go on the offensive against terrorism.

- The submission outlined our Counterterrorist Center's (CTC's) offensive operations, listing as their goals to "render the masterminds, disrupt terrorist infrastructure, infiltrate terrorist groups, and work with foreign partners."
- It highlighted efforts to work with the FBI in a bold program to destroy the infrastructure of major terrorist groups worldwide.
- The FY 1999 submission—prepared in early 1998—continued the trend in requesting a substantial funding increase for offensive operations against terrorism.
- The FY 2000 budget submission prepared in early 1999 described Bin Ladin as "the most significant individual sponsor of Sunni Islamic extremist and terrorist activity in the world today." Our FY 2000 submission noted our use of a wide range of operational techniques, joint operations with foreign partners, and the recruitment of well-placed agents.
- Commenting on the Bin Ladin-dedicated Issue Station in CTC, the FY 2000 submission noted that, "This Station, staffed with CIA, FBI, DOD, and NSA officers, has succeeded in identifying assets and members of Bin Ladin's organization, and nearly 700 intelligence reports have been disseminated about his operations."

Despite these clear intentions, and the daring activities that went with them, I was not satisfied that we were doing all we could against this target. In 1998, I told key leaders at CIA and across the Intelligence Community that we should consider ourselves

"at war" with Usama Bin Ladin. I ordered that no effort or resource be spared in prosecuting this war. In early 1999, I ordered a baseline review of CIA's operational strategy against Bin Ladin.

In spring 1999, CTC produced a new comprehensive operational plan of attack against the Bin Ladin/al-Qa'ida target inside and outside Afghanistan.

- This new strategy was previewed to senior CIA management by the end of July 1999. By mid-September, it had been briefed to CIA operational level personnel, and to NSA, the FBI, and other partners.

- CIA then began to put in place the elements of this operational strategy, which structured the Agency's counterterrorist activity until September 11th, 2001.

This strategy—which we called ***"The Plan"***—built on what CTC was recognized as doing well—collection, quick reaction to operational opportunities, renditions, disruptions, and analysis. Its priority was plain: to capture and bring to justice Bin Ladin and his principal lieutenants.

- The Plan included a strong and focused intelligence collection program to track—and then act against—Bin Ladin and his associates in terrorist sanctuaries. It was a blend of aggressive human source collection—both unilateral and with foreign partners—and technical collection.

- To execute the Plan, CTC developed a program to select and train the right officers and put them in the right places. We moved talented and experienced officers into the Center. We also initiated a nation-wide program to identify, vet and hire qualified personnel for counterterrorist assignments in hostile environments. We sought native fluency in the languages of the Middle East and South Asia, combined with police, military, business, technical, or academic experience. In addition, we established an eight-week advanced Counterterrorist Operations Course to share the tradecraft we had developed and refined over the years.

The parts of "the Plan" focused on Afghanistan faced some daunting impediments (some of which would change after 9/11). For example:

- The US Government had no official presence in Afghanistan, and relations with the Taliban were seriously strained. Both factors made it more difficult to gain access to Bin Ladin and al-Qa'ida personnel.

- US policy stopped short of replacing the Taliban regime, limiting the ability of the US Government to exert pressure on Bin Ladin.

- US relations with Pakistan, the principal access point to Afghanistan, were strained by the Pakistani nuclear tests in 1998 and the military coup in 1999.

Collection Profile

Despite these facts, our surge in collection operations paid off.

- Our human intelligence (HUMINT) reporting on the difficult Bin Ladin/al-Qa'ida target increased from roughly 600 reports in 1998 to 900 reports in the first nine months of 2001.

- Our HUMINT sources against the terrorism target grew by more than 50 percent between 1999 and 9/11.

- Working across agencies, and in some cases with foreign services, we designed and built several collection systems for specific use against al-Qa'ida inside Afghanistan.

- By 9/11, a map would show that these collection programs and human networks were in place in such numbers to nearly cover Afghanistan. This array meant that, when the military campaign to topple the Taliban and destroy al-Qa'ida began last October, we were able to support it with an enormous body of information and a large stable of assets.

The realm of human source collection frequently is divided between "liaison reporting" (that which we get from cooperative foreign intelligence services) and "unilateral reporting" (that which we get from agents we run ourselves). Even before "the Plan," our vision for HUMINT on terrorism was simple: we had to get *more* of *both types*. The figures for both rose every year after 1998. And in 1999, *for the first time*, the volume of reporting on terrorism from unilateral assets exceeded that from liaison sources—a trend which has continued in subsequent years.

The integration of technical and human sources has been key to our understanding of—and our actions against—international terrorism. It was this combination—this integration—that allowed us years ago to confirm the existence of numerous al-Qa'ida facilities and training camps in Afghanistan.

- On a virtually daily basis, analysts and collection officers from NSA, NIMA, and CIA came together to interactively employ satellite imagery, communications information, and human source reporting.

- This integration also supported military targeting operations prior to September 11, including the cruise missile attack against the al-Qa'ida training camp complex in northeastern Afghanistan in August 1998. In addition, it helped to provide baseline data for the US Central Command's

target planning against al-Qa'ida facilities and infrastructure throughout Afghanistan.

Countering Al-Qa'ida's Global Presence

Even while targeting UBL and al-Qa'ida in their Afghan lair, we did not ignore its cells of terror spread across the globe. Especially in periods of peak threat reporting, we accelerated our work to shake up and destroy al-Qa'ida cells wherever we could find them.

- This took resources--operations officers, desk officers, analysts, translators -- throughout the Intelligence Community and law enforcement agencies.

- We also mobilized intelligence services around the globe.

By 1999, the intensive nature of our operations was disrupting elements of Bin Ladin's international infrastructure. We believe that our efforts dispelled al-Qa'ida's impression that it could organize and operate with impunity. Our operations sent the message that the United States was not only going after al-Qa'ida for crimes it had committed, but also was actively seeking out and pursuing terrorists from al-Qa'ida and other groups engaged in *planning future attacks* whenever and wherever we could find them.

- By 11 September, CIA (in many cases with the FBI) had rendered 70 terrorists to justice around the world.

During the Millennium threat period, we told senior policymakers to expect between five and fifteen attacks, both here and overseas. The CIA overseas and the FBI in the US organized an aggressive, integrated campaign to disrupt al-Qaida using human assets, technical operations, and the hand-off of foreign intelligence to facilitate FISA court warrants.

Over a period of months, there was close, daily consultation that included Director Freeh, the National Security Adviser, and the Attorney General. We identified 36 additional terrorist agents at the time around the world. We pursued operations against them in 50 countries. Our disruption activities succeeded against 21 of these individuals, and included arrests, renditions, detentions, surveillance, and direct approaches.

- We assisted the Jordanian government in dealing with terrorist cells that planned to attack religious sites and tourist hotels. We helped track down the organizers of these attacks and helped render them to justice.

- We mounted disruption and arrest operations against terrorists in 8 countries on four continents, which also netted information that allowed us to track down even more suspected terrorists.

- During this same period, unrelated to the Millennium threats, we conducted multiple operations in East Asia, leading to the arrest or detention of 45 members of the Hizballah network.

- In the months after the Millennium experience—in October 2000—we lost a serious battle, when USS Cole was bombed and 17 brave American sailors perished.

The efforts of American intelligence to strike back at a deadly enemy continued through the Ramadan period in the winter of 2000, another phase of peak threat reporting.

- Terrorist cells planning attacks against US and foreign military and civilian targets in the Persian Gulf region were broken up, capturing hundreds of pounds of explosives and other weapons—including anti-aircraft missiles. These operations also netted proof that some Islamic charitable organizations had been either hijacked or created to provide support to terrorists operating in other countries.

- We succeeded in bringing a major Bin Ladin terrorist facilitator to justice with the cooperation of two foreign governments. This individual had provided documents and shelter to terrorists traveling through the Arabian Peninsula.

- We worked with numerous European governments, such as the Italians, Germans, French, and British to identify and shatter terrorist groups and plans against American and local interests in Europe.

Fusion and Sharing—the Intelligence Community and Law Enforcement

Taking the fight to Bin Ladin and al-Qa'ida was not just a matter of mobilizing CTC, or even CIA. This was an interagency—and international—effort. Two things which are critical to this effort are: fusion and sharing.

- The Counterterrorist Center (CTC) at CIA was created in 1986 to enable the fusion of all sources of information in a single, action-oriented unit. Not only do we fuse every source of reporting on terrorists from US and foreign collectors, we also fuse analysis and operations. This fusion gives us the speed that we must have to seize fleeting opportunities in the shadowy world of terrorism. Based on this proven philosophy, by 2001 the Center had more than 30 officers from more than a dozen agencies on board, ten percent of its staff complement at that time.

- No matter how much is fused within CTC, no matter how large CTC may be, there are still key counterterrorist players outside it, making the sharing of knowledge essential. Interview anyone in CTC, and he or she will likely tell you of work they are doing with counterparts across CIA—especially in the field—or with NSA, NIMA, FBI, or today with a Special Forces unit in Kandahar or Bagram.

It is also clear that, when errors occur—when we miss information or opportunities—it is often because our sharing and fusion are not as strong as they need to be. Communication across bureaucracies, missions, and cultures is among our most persistent challenges in the fast-paced, high-pressure environment of counterterrorism. I will return to this issue later in my testimony when I present some prescriptions for the future.

One of the most critical alliances in the war against terrorism is that between CIA and FBI. This alliance in the last few years has produced achievements that simply would not have been possible if some of the recent media stories of all-out feuding were true.

- An FBI officer has been serving as deputy to the Chief of CTC since the mid-1990s, and FBI reciprocated by making a CIA officer deputy in the Bureau's Counter-Terrorist Division.

- In the Bin Ladin Issue Station itself, FBI officers were detailed there soon after it opened in 1996, with the presence growing to four officers by September 2001.

There are abundant examples of close FBI-CIA partnership in counterterrorism.

- After the first World Trade Center bombing, FBI headed the investigation and CTC created an interagency task force to develop intelligence leads for the FBI. At FBI request, CIA obtained intelligence from a foreign service on Ramzi Yousef, who subsequently was convicted for the attack.

- After we received a rash of reports in 1998 threatening attacks in the United States, CIA worked together with FBI to provide advisories for local law enforcement agencies. One such episode occurred when CIA provided reporting of a plot to hijack a plane on the east coast of the United States to attempt to free the "Blind Shaykh" from prison. The report also said that there had been a successful test to elude security at a major airport.

- Also in 1998, FBI and CIA worked closely in the wake of the East Africa bombings to disrupt a planned attack on another U.S. Embassy in Africa. In a three-day period, more than 20 al-Qa'ida operatives were arrested in that country.

Of course, the relationship is not perfect, and frictions occasionally arise. A 1994 CIA Inspector General report noted that interactions between the two organizations were too personality dependent. This has been particularly so when the two were pursuing different missions in the same case: FBI trying to develop a case for courtroom prosecution, and CIA trying to develop intelligence to assess and counter a threat.

- In 2001 (before 9/11), the CIA IG found significant improvement, citing, for example, the Center's assistance to the FBI in two dozen renditions in 1999-2000.

- Director Freeh and I worked on this very hard. We had quarterly meetings of our senior leadership teams. Through training and other means, coordination between our Chiefs of Station overseas and legal attaches was significantly improved. Today, Bob Mueller and I are working to deepen our cooperation, not only at headquarters, but in the field. We both understand that despite different missions and cultures, we need to build a system of seamless cooperation that is institutionalized.

Increasing the difficulty of inter-agency communications is an unfortunate phenomenon known as "the Wall." It has been mentioned before in these hearings—the complex system of laws and rules (and perceptions about them) that impede the flow of information between the arenas of intelligence and criminal prosecution. The "Wall" slows and sometimes stops the flow of information—something we simply cannot afford. The Patriot Act has helped alleviate this.

Runup to 9/11—Our Operations

The third period of peak threat was in the spring and summer 2001. As with the Millennium and Ramadan 2000, we increased the tempo of our operations against al-Qa'ida. We stopped some attacks and caused the terrorists to postpone others.

- We helped to break up another terrorist cell in Jordan and seized a large quantity of weapons, including rockets and high explosives.

- Working with another foreign partner, we broke up a plan to attack US facilities in Yemen.

- In June, CIA worked with a Middle Eastern partner to arrest two Bin Ladin operatives planning attacks on US facilities in Saudi Arabia.

- In June and July, CIA launched a wide-ranging disruption effort against Bin Ladin's organization, with targets in almost two-dozen countries. Our intent was to drive up Bin Ladin's security concerns and lead his organization to delay or cancel its attacks. We subsequently received reporting that attacks were delayed, including an attack against the US

military in Europe.

- In July, a different Middle East partner helped bring about the detention of a terrorist who had been directed to begin an operation to attack the US Embassy or cultural center in European capital.

- Also in the summer of 2001, local authorities, acting on our information, arrested an operative described as Bin Ladin's man in East Asia.

- We assisted another foreign partner in the rendition of a senior Bin Ladin associate. Information he provided included plans to kidnap Americans in three countries, and carry out hijackings.

- We provided intelligence to a Latin American service on a band of terrorists considering hijackings and bombings. An FBI team detected explosives residue in their hotel rooms.

Runup to 9/11—the Watchlist Issue

During the period of the Millennium threats, one of our operations, and one of our mistakes, occurred during our accelerating efforts against Bin Ladin's organization—when we glimpsed two of the individuals who later became 9/11 hijackers, Khalid al-Mihdhar and Nawaf al-Hazmi.

- In December 1999, CIA, FBI, and the Department of State received intelligence on the travels of suspected al-Qa'ida operatives to Kuala Lumpur, Malaysia. CIA saw the Kuala Lumpur gathering as a potential source of intelligence about a possible al-Qa'ida attack in Southeast Asia. We initiated an operation to learn why those suspected terrorists were traveling to Kuala Lumpur. Khalid and Nawaf were among those travelers, although at the time we knew nothing more about them except that Khalid had been at a suspected al-Qa'ida logistics facility in Yemen. We arranged to have them surveilled.

- In early January 2000, we managed to obtain a photocopy of al-Mihdhar's passport as he traveled to Kuala Lumpur. It showed a US multiple-entry visa issued in Jeddah on 7 April 1999 and expiring on 6 April 2000. We learned that his full name is Khalid bin Muhammad bin 'Abdallah al-Mihdhar.

- We had at that point the level of detail needed to watchlist him—that is, to nominate him to State Department for refusal of entry into the US or to deny him another visa. Our officers remained focused on the surveillance operation, and did not do this.

At this early stage, the first days of January 2000, CIA briefed the FBI, informally, about the surveillance operation in Kuala Lumpur. We noted in an internal CIA communication on 5 January 2000 that we had passed a copy of al-Mihdhar's passport—*with its US visa*—to the FBI for further investigation. A CTC officer at the FBI wrote an e-mail in January 2000 reporting that he briefed FBI officers on the surveillance operation, noting suspicious activity but no evidence of an impending attack.

The relative importance of al-Mihdhar and al-Hazmi at this time should be kept in perspective. Neither al-Mihdhar nor al-Hazmi at the time of their travel to Kuala Lumpur were identified as key al-Qa'ida members or associates. Thus, at this point, their significance to us was that they might lead us to others or to threat information. During this period when all CIA facilities were involved in dealing with the Millennium Threat, there was particular CTC focus on three separate groups of al-Qa'ida personnel:

- Those known to have been already involved in a terrorist attack such as the East Africa embassy bombings, or suspected of being involved in planning a reported attack (e.g., East Africa embassy bombing suspect Abdul Rahman al-Muhajir);

- Senior al-Qa'ida personnel outside Afghanistan known to be directors or coordinators of terrorist operations, or senior money couriers, liaison officers or manipulators of NGO's and businesses supporting terrorist groups (e.g., terrorist operational planner Abu Zubaydah); and

- Senior al-Qa'ida personnel inside Afghanistan, particularly those close to Bin Ladin who might know of his attack or travel plans (e.g., Bin Ladin deputy Muhammad Atef).

Surveillance began with the arrival of Khalid al-Mihdhar on 5 January 2000, and ended on 8 January, when he left Kuala Lumpur. Surveillance indicated that the behavior of the individuals was consistent with clandestine activity—they did not conduct any business or tourist activities while in Kuala Lumpur, and they used public telephones and cyber cafes exclusively.

Other individuals were also positively identified by the surveillance operation.

- Later in 2001 an individual was identified as Saeed Muhammad Bin Yousaf (aka Khallad), who became a key planner in the October 2000 USS Cole bombing. Because of his later connection with the Cole bombing and other serious plotting, we believe he was the most important figure to attend the Kuala Lumpur meeting.

- Another individual identified by surveillance was Malaysian citizen Ahmad Sajuli Abdul Rahman. During the period, 6-8 January, Sajuli took the al-Qa'ida visitors around Kuala Lumpur. Two years later, Sajuli has

been arrested and has admitted being part of the logistics unit for Jemaah Islamiah, an affiliate of al-Qa'ida.

- Yazid Sufaat, a Malaysian chemist who, it was later determined, was directed by a terrorist leader to make his apartment available to the al-Qa'ida operatives. He is now under arrest.

- Sufaat's name would later be connected to that of Zacarias Moussaoui.

To this day, we still do not know what was discussed at the Kuala Lumpur meeting. Al-Mihdhar and al-Hazmi remained there a few days. On 8 January 2000, they traveled to another Southeast Asian country with Khallad. We learned in March 2000 that al-Hazmi flew from that country to Los Angeles on January 15, 2000. We did not learn that al-Midhar was on the same flight until August, 2001.

- Our receipt of the information in March should have triggered the thought to watchlist al-Hazmi, but no CTC officer recalls even having seen the cable on his travel to LA when it arrived.

Al-Mihdhar departed the US on 10 June 2000 and obtained a new passport and US visa, possibly for operational security reasons. Al-Mihdhar applied for this new US visa in Jeddah in 13 June and stated that he had never traveled to the US before. On 4 July 2001, he returned to the US, entering in New York.

During August 2001, CIA had become increasingly concerned about a major terrorist attack on US interests, and I directed a review of our files to identify potential threats. CTC reviewed its holdings on al-Mihdhar because of his connections to other terrorists. In the course of that review, CTC found that al-Mihdhar and al-Hazmi had entered the US on 15 January 2000. It determined that al-Mihdhar departed the US on 10 June 2000 and reentered on 4 July 2001. CTC found no record of al-Hazmi's departure from the US.

- On 23 August, CIA sent a message—marked "immediate"—to the Department of State, INS, Customs, and the FBI requesting to enter al-Mihdhar and al-Hazmi, Bin Ladin-related individuals, into VISA/VIPER, TIPOFF and TECS. The message said that CIA recommends that al-Mihdhar and al-Hazmi be watchlisted immediately.

There are at least two points before August 2001 when these individuals were on our scope with sufficient information to have been watchlisted. During the intense operations to thwart the Millennium and Ramadan threats, the watchlist task in the case of these two al-Qaida operatives slipped through. The error exposed a weakness in our internal training and an inconsistent understanding of watchlist thresholds. Corrective steps have been taken.

- The CIA and the State Department are cooperating to transform the TIPOFF all-source watchlist into a National Watchlist Center. This center will serve as the point of contact and coordination for all watchlists in the U.S. Government.

- We have increased managerial review of the system to reduce the chance that watchlist opportunities will be missed in the crush of other urgent business.

- We have designed a database and assembled a team to consolidate information on the identities of known and suspected terrorists, and to flag any that has not been passed to the proper audience.

- We have lowered the threshold for nominating individuals for the watchlist and clarified that threshold for our officers

- We have lowered the threshold for dissemination of information that used to be held closely as "operational."

These corrective steps notwithstanding, we must not underestimate our enemies' capabilities.

- We know that the plot was extremely resilient.

- We know that al-Qa'ida deliberately chose young men who had no record of affiliation with terrorist activities; 17 of the 19 hijackers were clean in this respect.

- We know that al-Hazmi and al-Mihdhar tried to become pilots but abandoned the effort because of poor technical and English language skills. By the end of 2000, a replacement pilot for Flight 77, Hani Hanjur, was in the United States.

- We know that Ramzi bin Al-Shib tried on multiple occasions to get into the US and failed, and yet the plot continued.

- Finally, we know that Zacarias Moussaoui was arrested but refused to provide information on the plot.

Runup to 9/11—the Warning Issue

In the months leading up to 9/11, we were convinced Bin Ladin meant to attack Americans, meant to kill large numbers, and that the attack could be at home, abroad, or both. And we reported these threats urgently.

Our collection sources "lit up" during this tense period. They indicated that multiple spectacular attacks were planned, and that some of these plots were in the final stages.

- Some of the reporting implicated known al-Qaida operatives.
- The reports suggested that the targets were American, although some reporting simply pointed to the West or Israel.
- But the reporting was maddeningly short on actionable details. The most ominous reporting, hinting at something large, was also the most vague. The only occasions in this reporting where there was a geographic context, either explicit or implicit, it appeared to point abroad, especially to the Middle East.
- By long established doctrine, we disseminated these raw reports immediately and widely to policymakers and action agencies such as the military, State Department, the FAA, FBI, Department of Transportation, the INS, and others.
- This reporting, by itself, stood as a dramatic warning of imminent attack.

Our analysts worked to find linkages among the reports, as well as links to past terrorist threats and tactics. We considered whether al-Qa'ida was feeding us this reporting—trying to create panic through disinformation—yet we concluded that the plots were real. When some reporting hinted that an attack had been delayed, we continued to stress that there were, indeed, multiple attacks planned and that several continued on track. And when we grew concerned that so much of the evidence pointed to attacks overseas, we noted that Bin Ladin's principal ambition had long been to strike our homeland. Nevertheless with specific regard to the 9/11 plot, we never acquired the level of detail that allowed us to translate our strategic concerns into something we could act on.

The Intelligence Community Counterterrorism Board also issued several threat advisories during the summer 2001. These advisories—the fruit of painstaking analytical work—contained phrases like "al-Qa'ida is most likely to attempt spectacular attacks resulting in numerous casualties," and "al-Qa'ida is prepared to mount one or more terrorist attacks at any time."

A sign that our warnings were being heard—both from our analysis and from the raw intelligence we disseminated—was that the FAA issued two alerts to air carriers in the summer of 2001.

Our warnings complemented strategic warnings we had been delivering for years about the real threat of terrorism to America.

- Recall, Mr. Chairman, my testimony in open session before your committee on February 2, 1999 when I told you "there is not the slightest doubt that Usama Bin Ladin, his worldwide allies, and his sympathizers are planning further attacks against us." I told you "he will strike wherever in the world he thinks we are vulnerable" and that we were "concerned that one or more of Bin Ladin's attacks could occur at any time."

- In February 2000, I testified in open session that, "Everything we have learned recently confirms our conviction that (UBL) wants to strike further blows against America" and that he could strike "without additional warning."

- Again in 2001 I told you that "terrorists are seeking out 'softer' targets that provide opportunities for mass casualties" and that Bin Ladin is "capable of planning multiple attacks with little or no warning."

- In a National Intelligence Estimates in 1995 we warned, *"As an open and free democracy, the United States is particularly vulnerable to various types of terrorist attacks. Several kinds of targets are especially at risk: National symbols such as the White House and the Capitol, and symbols of US capitalism such as Wall Street; power grids, communications switches, water facilities, and transportation infrastructure—particularly civil aviation, subway systems, cruise lines, and petroleum pipelines; places where large numbers of people congregate, such as large office buildings, shopping centers, sports arenas, and airport and other transportation terminals."*

- The same estimate also said, *"We assess that civil aviation will figure prominently among possible terrorist targets in the United States. This stems from the increasing domestic threat posed by foreign terrorists, the continuing appeal of civil aviation as a target, and a domestic aviation security system that has been the focus of media attention: We have evidence that individuals linked to terrorist groups or state sponsors have attempted to penetrate security at US airports in recent years. The media have called attention to, among other things, inadequate security for checked baggage. Our review of the evidence obtained thus far about the plot uncovered in Manila in early 1995, suggests the conspirators were guided in their selection of the method and venue of attack by carefully studying security procedures in place in the region. If terrorists operating in this country are similarly methodical, they will identify serious vulnerabilities in the security system for domestic flights."*

- In a National Intelligence Estimate in 1997, we said *"Civil aviation remains a particularly attractive target for terrorist attacks in light of the fear and publicity the downing of an airliner would evoke and the revelations last summer of the vulnerability of the US air transport sector."*

Message Received

In February 1997, the White House Commission on Aviation Safety and Security reported that:

> *"The Federal Bureau of Investigation, the Central Intelligence Agency, and other intelligence sources have been warning that the threat of terrorism is changing in two important ways. First, it is no longer just an overseas threat from foreign terrorists. People and places in the United States have joined the list of targets, and Americans have joined the ranks of terrorists. The bombings of the World Trade Center in New York and the Federal Building in Oklahoma City are clear examples of the shift, as is the conviction of Ramzi Yousef for attempting to bomb twelve American airliners out of the sky over the Pacific Ocean. The second change is that in addition to well-known, established terrorist groups, it is becoming more common to find terrorists working alone or in ad-hoc groups, some of whom are not afraid to die in carrying out their designs."*

In its publication, "Criminal Acts against Civil Aviation 2000," the FAA stated:

> *"Although Bin Ladin is not known to have attacked civil aviation, he has both the motivation and the wherewithal to do so. Bin Ladin's anti-Western and anti-American attitudes make him and his followers a significant threat to civil aviation, especially U.S. civil aviation."*

In discussing the plot by convicted World Trade Center bomber Ramzi Yousef to place explosive devices on as many as 12 U.S. airliners flying out of the Far East, the FAA's report points out that at least one other accused participant in the conspiracy remains at large, and:

> *"There are concerns that this individual or others of Yousef's ilk who may possess similar skills pose a continuing threat to civil aviation interests...Increased awareness and vigilance are necessary to deter future incidents -- be they from terrorists or non-terrorists. It is important to do the utmost to prevent such acts rather than to lower security measures by interpreting the statistics as indicating a decreasing threat."*

We have heard the allegation that our analysts erred by not explicitly warning that hijacked aircraft might be used as weapons. Your staff has been given access to over half a million pages of documents and interviewed hundreds of intelligence officials in their efforts to investigate this complex issue. The documents we provided show some 12 reports, spread over seven years, which pertain to possible use of aircraft as weapons in terrorist attacks.

- We disseminated those reports to the appropriate agencies—such as the FAA, Department of Transportation, and FBI—as they came in. Moreover, we also provided sanitized versions of intelligence reports that were about threats to civil aviation so they could be distributed more widely through the airline industry.

- But if one goes back and collects the reports over the same period that pertained to possible truck bombs, car bombs, assassinations, kidnappings, or attacks using chemical, biological, radiological or nuclear devices, those lists would have been far longer. A quick scan of such reporting since 1996, for example, showed about 20 times as many reports concerning car bombs and about five times as many reports concerning weapons of mass destruction.

BUDGET AND RESOURCES

To evaluate our work on al-Qa'ida before 9/11 objectively, it is essential that you look at three issues: global geopolitical issues we were grappling with -- including counterterrorism; resource changes throughout the 1990s that affected our ability to fight the counterterrorism fight; and the overall health of US intelligence during this period. It is simply not enough to look at al-Qa'ida in isolation.

The last decade saw a number of conflicting and competing trends: military forces deployed to more locations than ever in our nation's history; a growing counterproliferation and counterterrorism threat; constant tensions in the Mid East and, to deal with these and a host of other issues, far fewer intelligence dollars and manpower. At the end of the Cold War, the Intelligence Community, like much of the National Security Community, was asked by both Congress and successive Administrations to pay the price of the "peace dividend."

The cost of the "peace dividend" was that during the 1990s our Intelligence community funding declined in real terms – reducing our buying power by tens of billions of dollars over the decade. We lost nearly one in four of our positions. This loss of manpower was devastating, particularly in our two most manpower intensive activities: all-source analysis and human source collection. By the mid-1990s, recruitment of new CIA analysts and case officers had come to a virtual halt. NSA was hiring no new technologists during the greatest information technology change in our

lifetimes. It is absolutely essential that we understand that both Congress and the Executive Branch for most of the decade embraced the idea that we could "surge" our resources to deal with emerging intelligence challenges, including threats from terrorism. And surge we did.

- As I "declared war" against al-Qa'ida in 1998 – which was in the aftermath of the East Africa embassy bombings – we were in our fifth year of round-the-clock support to Operation Southern Watch in Iraq.

- Just three months earlier, we were embroiled in answering questions on the India and Pakistan nuclear tests and trying to determine how we could surge more people to understanding and countering weapons of mass destruction proliferation.

- In early 1999, we surged more than 800 analysts and redirected collection assets from across the Intelligence Community to support the NATO bombing campaign against the Federal Republic of Yugoslavia.

During this time of increased military operations around the globe, the Defense Department was also reducing its tactical intelligence units and funding. This caused the Intelligence Community to stretch our capabilities to the breaking point – because national systems were covering the gaps in tactical intelligence. It is always our policy to give top priority to supporting military operations.

While we grappled with this multitude of high priority, overlapping crises, we had no choice but to modernize selective intelligence systems and infrastructure in which we'd deferred necessary investments while we downsized – or we would have found ourselves out of business. We had a vivid example of the cost of deferring investments a few years ago when NSA lost all communications between the headquarters and its field stations and we were unable to process any of that information for several days. We have a more current example of the cost of deferred investments today as we struggle to recapitalize our aging satellite constellation -- another "return" on the peace dividend, given that conscious decisions to accept risk and defer replacing these systems were made in the mid-1990s. At the same time, we added the National Imagery and Mapping Agency to the Intelligence Community along with enormous funding shortfalls required to merge and modernize its geospatial and imagery functions.

Throughout the Intelligence Community during this period we made difficult resource reallocation decisions to try to rebuild critical mission areas affected by the funding cuts. For example,

- In CIA we launched a program to rebuild our Clandestine Service. This meant overhauling our recruitment and training practices and our infrastructure. We launched similar initiatives to rebuild our analytic depth and expertise, and to re-acquire our leading edge in technology.

Although we will not be given credit for these efforts in the war on terrorism, they most assuredly contributed to that effort.

- NSA made the hard decision to cut additional positions to free up pay and benefit dollars to patch critical infrastructure problems and to modestly attempt to capitalize on the technology revolution.

But with the al-Qa'ida threat growing more ominous, and with our resources devoted to countering it clearly inadequate, we began taking money and people away from other critical areas to improve our efforts against terrorism.

Despite the resource reductions and the enormous competing demands for our attention, we managed to triple Intelligence Community-wide funding for counterterrorism from fiscal year 1990 to 1999. The Counterterrorism Center's resources nearly quadrupled in that same period. As your own Joint Inquiry Staff charts show, we had significantly reallocated both dollars and people inside our programs to work the terrorism problem. This inquiry has singled out CIA resources specifically and I want to address it specifically.

From a budget perspective, the last part of the 1990s reflects CIA's efforts to shift to a wartime footing against terrorism. CIA's budget had declined 18 percent in real terms during the decade and we suffered a loss of 16 percent of our personnel. Yet in the midst of that stark resource picture, CIA's funding level for counterterrorism just prior to 9/11 was more than 50 percent above our FY 1997 level. CTC personnel increased by over 60% for that same period. The CIA consistently reallocated and sought additional resources for this fight. In fact, in 1994, the budget request for counterterrorism activities equaled less than four percent of the total CIA program. In the FY 2002 CIA budget request we submitted prior to 9/11, counterterrorism activities constituted almost 10 percent of the budget request. During a period of budget stringency when we were faced with rebuilding essential intelligence capabilities, I had to make some tough choices. Although resources for virtually everything else in CIA was going down, counterterrorism resources were going up.

But after the US embassies in Africa were bombed, we knew that neither surging our resources nor internal realignments were sufficient to fund a war on terrorism. So in the fall of 1998, I asked the Administration to increase intelligence funding by more than $2.0 billion annually for fiscal years 2000-2005 and I made similar requests for FY 2001-2005 and FY 2002-2007. Only small portions of these requests were approved. Counterterrorism funding and manpower needs were number one on every list I provided to Congress and the Administration and, indeed, it was at the top of the funding list approved by Speaker Gingrich in FY1999, the first year in which we received a significant infusion of new money for US intelligence capabilities during the decade of the 90s.

That supplemental and those that followed it, that you supplied, were essential to our efforts – they helped save American lives. But we knew that we could not count on

supplemental funds to build multi-year programs and that's why we worked so hard to reallocate our resources and to seek five year funding increases. Many of you on this Committee and the Appropriations Committees understood this problem very well. You were enormously helpful to us. And we are grateful.

I want to conclude with a couple of comments about manpower. In CIA alone, I count the equivalent of 700 officers working counterterrorism in August 2001 at both headquarters and in the field. That number does not include the people who were working to penetrate either technically or through human sources a multitude of threat targets from which we could derive intelligence on terrorists. Nor does it include friendly liaison services and coalition partners. You simply cannot gauge the level of effort by counting only the people who had the words "al-Qa'ida" or "bin Ladin" in their position description.

We reallocated all the people we could given the demands placed on us for intelligence on a number of the highest priority issues like chemical, nuclear and biological proliferation and support to operational military forces, and we surged thousands of people to fight this fight when the threat was highest. But when we realized surging wasn't sufficient, we began a sustained drumbeat both within the Administration and here on the Hill that we had to have more people and money devoted to this fight.

We can argue for the rest of the day about the exact number of people we had working this problem but what we never said, was that the numbers we had were enough. Our officers told your investigators that they were always shorthanded. They were right. America may never know the names of those officers, but America should know they are heroes. They worked tirelessly for years to combat bin Ladin and al-Qa'ida and have responded to the challenge of combating terrorism all during this time, with remarkable intensity. Their dedication, professionalism and creativity stopped many al-Qa'ida plots in their tracks – they saved countless American lives. Most of them are still in this fight – are essential to this fight – and they honor us by their continued service.

Thanks to the last two emergency supplementals and the Administration's FY03 budget request, which both Houses approved during the past week, we have begun to move aggressively to reverse the funding shortfalls that have had such an impact on the nation's intelligence capabilities. But we have hardly scratched the surface in our efforts to recover from the manpower reductions, and we cannot reconstitute overnight the cadre of seasoned case officers and assets overseas, or the expert team of analysts we've lost. It will take many more years to recover from the capabilities we lost during the resource decline of the 1990s.

FINAL OBSERVATIONS

Success against the terrorist target must be measured against all elements of our nation's capabilities, policies and will. The intelligence community and the FBI are important parts of the equation, but by no means the only parts. We need a national,

integrated strategy in our fight against terrorism that incorporates both offense and defense. The strategy must be based on three pillars:

- Continued relentless effort to penetrate terrorist groups, whether by human or technical means, whether alone or in partnership with others.

- Second, intelligence, military, law enforcement, and diplomacy must stay on the offense continually against terrorism around the world. We must disrupt and destroy the terrorists' operational chain of command and momentum, deny them sanctuary anywhere and eliminate their sources of financial and logistical support.

  Nothing did more for our ability to combat terrorism than the President's decision to send us into the terrorist's sanctuary. By going in massively, we were able to change the rules for the terrorists. Now they are the hunted. Now they have to spend most of their time worrying about their survival. Al-Qa'ida must never again acquire a sanctuary.

- Third, on defense, we need systematic security improvements to protect our country's people and infrastructure and create a more difficult operating environment for terrorists. The objective is to understand our vulnerabilities better than the terrorist do, take action to reduce those vulnerabilities, to increase the costs and risks for terrorists to operate in the United States and, over time, make those costs unacceptable to them.

We have learned an important historic lesson: We can no longer race from threat to threat, resolve it, disrupt it *and then move on. Targets at risk remain at risk.*

- In 1993, the first attack on the World Trade Center did, in comparative terms, modest damage. A plot around the same time to attack New York City tunnels and landmarks was broken up. We all breathed a sigh of relief and moved on, focusing the effort mostly on bringing perpetrators to justice. *The terrorists came back.*

- At the Millennium, a young terrorist panicked at a Canada-US border crossing and his plan to attack an airport in Los Angeles was exposed and thwarted. We breathed another sigh of relief and prepared for his trial. *Al Qa'ida's plan has only been delayed.*

- Last winter, another young terrorist on an airliner ineptly tried to detonate explosives in his shoes and was stopped by alert crew and passengers. At this point, we're smarter—we started checking everyone's shoes for explosives. *It is not nearly enough.*

- In the last year, we have gone on high alert several times for good reason, only to have no attack occur. We all breathed a sigh of relief and thought, "maybe it was a false alarm." *It wasn't.*

- *We must design systems that reduce both the chances of an attack getting through and its impact if it does. We must address both the threat and our vulnerability. We must not allow ourselves to mentally "move on" while this enemy is still at large.*

I strongly support the President's proposal to create a Department of Homeland Security. The nation very much needs the single focus that this department will bring to homeland security. We have a foreign intelligence community and law enforcement agencies, but we have not had a cohesive body responsible and empowered for homeland security. The President's proposal closes that gap while building bridges between all three communities.

- The Department's most important role will be to correlate threat warnings and assessments about evolving terrorist strategies with a fine-grained understanding of the vulnerabilities of all sectors of the homeland and translate that into a ***system*** of protection for the people and infrastructure of the United States.

While the Department will be vital to our homeland defense, the most valued resource for our work against terrorism has always been and will forever be our people.

Moving from this necessary organizational change, I cannot emphasize enough our overwhelming need to recruit and train the intelligence officers we need to win this war.

Terrorists have a tactical advantage. They can pick and choose any target they please, who are willing to sacrifice their lives, and who don't care how many innocents they hurt or kill have tactical advantage. Developing the intelligence to combat them is manpower intensive. With the personnel we have invested in counterterrorism today, we can do much more than we could before 9/11, but more are still needed. I remind you that we lost nearly 1-in-4 of our positions since the end of the Cold War.

Our people also need better ways to communicate. Moreover, we also need systems that enable us to share critical information quickly across bureaucratic boundaries. Systems to put our intelligence in front of those who need it wherever they may be, whatever their specific responsibilities for protecting the American people from the threat of terrorist attack. That means we must move information in ways and to places it has never before had to move. We are improving our collaborative systems. We need to improve our multiple communications links--both within the Intelligence Community and now in the Homeland Security community as well. Building, maintaining, and constantly updating this system will require a massive, sustained budget infusion, separate from our other resource needs.

Now, more than ever before, we need to make sure our customers get from us exactly what they need -- which generally means exactly what they want -- fast and free of unnecessary restrictions. Chiefs of police across the country express understandable frustration at what they do not know. But there's something else: Intelligence officers in the federal government want to get their hands on locally collected data. Each could often use what the other may already have collected. The proposed Department of Homeland Security will help develop this vertical sharing of information. So, too, will the Intelligence Community's experience in supporting our armed forces. We're going to have to put that experience to work in "supporting the mayor." We don't have the luxury of an alternative.

One last point with regard to our human talent. As critical as terrorism is, our people will not concentrate solely on counterterrorism. Even in the last year, when national attention was focused on terror, other events occurred which demanded the attention of experienced intelligence officers. The risk of an Indian-Pakistani war and the deterioration of the situation in the Mid East are just two examples. The Intelligence Community must keep skilled, experienced officers on all such issues.

CONCLUDING STATEMENT

Our effectiveness has increased since September 11, and the Intelligence Community will continue to pursue a strategy of bringing the war to the terrorists.

But in the counterterrorism business there is no such thing as 100 percent success—there will never be.

- Some of what terrorists plan and do will remain hidden. The al Qa'ida practice is to keep their most lethal plots within a small, tightly knit group of fanatics. This is not an *impossible* target, but it is among our *hardest.*

- Total success against such targets is impossible. Some attackers will continue to get through us.

It may be comforting on occasion to think that if we could find the one process that went wrong, then we could remedy that failing and return to the sense of safety we enjoyed prior to 9/11. The reality is that we were vulnerable to suicidal terrorist attacks and we remain vulnerable to them today. That is not a pleasant fact for Americans to live with, but it is the case. There are no easy fixes. We will continue to look incisively at our own processes and to listen to others in an ongoing effort to do our jobs better. But we must also be honest with ourselves and with the public about the world in which we live.

The fight against international terrorism will be long and difficult.

- It will require the patience and diligence that the President has asked for.

- It will require resources—sustained over a multi-year period—to re-capitalize our intelligence infrastructure on a pace that matches the changing technical and operational environment we face.

- It will also require countries that have previously ignored the problem of terrorism or refused to cooperate with us to step up and choose sides.

It will require all of us across the government to follow the example of the American people after September 11 -- to come together, to work as a team, and pursue our mission with unyielding dedication and unrelenting fidelity to our highest ideals. We owe those who died on September 11 and all Americans no less.

TESTIMONY OF GEORGE TENET, DIRECTOR, CENTRAL INTELLIGENCE AGENCY

Director TENET. Mr. Chairman, thank you. I am not going to be able to get this done in ten minutes. We will try and be as fast as I can, but we have a lot that we have to say, and we will be as quick as I can. And I thank you for your indulgence in that regard.

I welcome the opportunity to be here today to be part of an inquiry that is vital to all Americans. On September 11, nearly 3,000 innocent lives were taken in brutal acts of terror. For the men and women of American intelligence, the grief we feel, the grief we share with so many others is only deepened by the knowledge of how hard we tried without success to prevent this attack.

It is important for the American people to understand what CIA and the Intelligence Community were doing to try to prevent the attacks that occurred and to stop future attacks which al-Qa'ida has certainly planned and remains determined to attempt.

What I want to do this morning, as explicitly as I can, is to describe the war we have waged for years against al-Qa'ida, the level of effort, the planning, the focus, and the enormous courage and discipline shown by our officers throughout the world.

It is important for the American people to understand how knowledge of the enemy translated into action around the globe, including the terrorist sanctuary of Afghanistan before September 11. It is important to put our level of effort into context, to understand the trade-offs in resources and people we had to make, the choices we consciously made to ensure that we maintained an aggressive counterterrorism effort.

We need to understand that in the field of intelligence long-term erosion of resources cannot be undone quickly when emergencies arise, and we need to explain the difference that sustained investments in intelligence, particularly in people, will mean for our country's future.

We need to be honest about the fact that our homeland is very difficult to protect. For strategic warning to be effective, there must be a dedicated program to address the vulnerabilities of our free and open society. Successive administrations, commissions, and the Congress have struggled with this. To me it is not a question of surrendering liberty for security but of finding a formula that gives us the security we need to defend the liberty that we treasure, not simply to defend it in a time of peace but to preserve it in a time of war, a war in which we must be ready to play offense and defense simultaneously.

That is why we must arrive soon at a national consensus on homeland security. We need to be honest about our shortcomings and tell you what we have done to improve our performance in the future.

There have been thousands of actions in this war, an intensely human endeavor, not all of which have been executed flawlessly. Nevertheless, the record will show a keen awareness of the threat, the disciplined focus and persistent efforts to track, disrupt, apprehend, and ultimately try to bring to justice bin Ladin and his lieutenants.

Somehow lost in much of the debate since September 11 is one unassailable fact: The U.S. Intelligence Community could not have

surged, as it has in the conflict in Afghanistan and engaged in an unprecedented level of operations around the world, if it were as mired as some have portrayed.

It is important for the American people to know that despite the enormous successes we have had in the past year, indeed over many years, al-Qa'ida continues to plan and will attempt more deadly strikes against us. There will be more battles won, and sadly more battles lost. We must be honest about that too.

Finally, we need to focus on the future and consider how the knowledge we have gained this year will be applied. Let me begin by describing the rise of Usama bin Ladin and the Intelligence Community's response. We recognized early on the threat posed by him and his supporters. As that threat developed, we tracked it, we reported it to the executive branch policymakers, Congress and, when feasible, directly to the American people.

We reacted to the growing threat by conducting energetic, innovative and increasingly risky operations to combat it. We went on the offensive. And this effort mattered. It saved lives, perhaps in the thousands. And it prepared the field for the rapid success in Afghanistan last winter.

The first rule of warfare is know your enemy. My full statement documents our knowledge and analysis of bin Ladin from his early years as a terrorist financier to his leadership of a worldwide network based in Afghanistan. But suffice it to say that as bin Ladin's prominence grew in the early 1990s it became clear to CIA that it was simply not enough to collect and report intelligence about him.

As early as 1993, our units watching him began to propose action to reduce his organization's capabilities. I must pause here. In an open forum, I cannot describe what authorities we sought or received. But it is important that the American people understand two things. The first is about covert action in general. CIA can only pursue such activities with the express authorization of the President.

The second point is that when such proposals are considered, it is always because we or policymakers, identify a threatening situation, a situation to which we must pay far greater attention, and one in which we must run far greater risks. As long ago as 1993, we saw such a situation with Usama bin Ladin. By the time bin Ladin left Sudan in 1996 and relocated himself and his terror network to Afghanistan, the Intelligence Community was taking action to stop him. We established a special unit known as the bin Ladin Issue Station, with CIA, NSA, FBI and other officers, specifically to get more and more actionable intelligence on bin Ladin and his organization.

We took this step because we knew the traditional approaches alone would not be enough for this target. We monitored his whereabouts, increased our knowledge about him and his organization with information from our own assets and from many foreign intelligence services. We were working hard on a program to disrupt his finances, degrade his ability to engage in terrorism, and ultimately to bring him to justice.

We must remember that, despite the heightened attention, bin Ladin was in the mid 1990s one of four areas of concentration within our counterterrorism center. That concentration included

Hizbollah, the Egyptian Islamic Jihad, al Gama'at, the Palestinian rejectionists and smaller groups around the world. Once bin Ladin found safe haven in Afghanistan, he defined himself publicly as a threat to the United States.

While we often talk of two trends in terrorism, state-supported and independent, in bin Ladin's case with the Taliban we had something completely new—a terrorist supporting a state. What bin Ladin created in Afghanistan was a sophisticated adversary, as good as any that we have ever operated against.

As the Intelligence Community improved its understanding of the threat, and as the threat grew, we refocused and intensified our efforts to track, disrupt and bring these terrorists to justice.

By 1998, the key elements of our strategy against bin Ladin and al-Qa'ida inside Afghanistan and globally placed us in a strongly offensive posture. They included hitting al-Qa'ida's infrastructure, working with our foreign partners to carry out arrests, disrupting and weakening his finances, recruiting or exposing operatives, pursuing a multi-track approach to bring bin Ladin himself to justice, working with foreign services, developing a close relationship with U.S. Federal prosecutors, increasing pressure on the Taliban and our enhancing our capabilities to capture him.

Our 1998 budget submission to the Congress, which was prepared in early 1997, outlined our Counterterrorism Center's offensive operations, listing as their goals to render the masterminds, disrupt terrorist infrastructure, infiltrate terrorists groups and work with foreign partners.

It highlighted efforts to work with the FBI in a bold program to destroy the infrastructure of major terrorist groups worldwide. In each subsequent year we delivered to you equally emphatic statements of our intent. Despite these clear intentions and the daring activities that went with them, I was not satisfied that we were doing all we could against this target.

In 1998 I told key leaders at CIA and across the Intelligence Community that we should consider ourselves at war with Usama bin Ladin. I ordered that no effort or resource be spared in prosecuting this war. In early 1999 I ordered a baseline review of CIA's operational strategy against bin Ladin.

In spring of 1999 we produced a new comprehensive operational plan of attack against him and al-Qa'ida inside and outside of Afghanistan. The strategy was previewed to senior CIA management by the end of July of 1999. By mid-September it had been briefed to the CIA operational level personnel, to NSA, to the FBI and other partners.

CIA began to put in place the elements of this operational strategy which structured the Agency's counterterrorism activity until September 11 of 2001. This strategy, which we call "the plan," builds on what our Counterterrorism Center was recognized as doing well—collection, quick reaction to operational opportunities, renditions, disruptions and analysis. Its priority was plain—to capture and bring bin Ladin and his principal lieutenants to justice.

The plan included a strong and focused intelligence collection program to track and act against bin Ladin and his associates in terrorist sanctuaries. It was a blend of aggressive human source

collection, both unilateral and with foreign partners, and enhanced technical collection.

To execute the plan——

Chairman GRAHAM. Mr. Tenet, ten minutes. If you want to proceed.

Director TENET. I would like to, sir. To execute the plan, CTC developed a program to select and train the right officers and put them in the right places. We moved talented and experienced operations officers into the center. We initiated a nationwide program to identify, vet and hire qualified personnel for counterterrorism assignments. We sought native fluency in the languages of the Middle East and South Asia, combined with police, military, business, technical, or academic expertise.

In addition, we established an eight-week advanced counterterrorism operations course to share the tradecraft we had developed and refined over the years. The parts of the plan that focused on Afghanistan faced some daunting impediments. U.S. policy stopped short of replacing the Taliban regime. U.S. relations with Pakistan, one of the principal access points, were strained by the Pakistani nuclear tests and the military coup in 1999.

Despite these facts, our surge in collection and operations paid off. Our human intelligence reporting grew. Our human intelligence sources against terrorism grew by more than 50 percent between 1999 and 9/11. Working across agencies, and in some cases with foreign services, we designed and built several collection systems for specific use against al-Qa'ida inside Afghanistan. By 9/11 a map would show that these collection programs and human networks were in place in such numbers as to nearly cover Afghanistan.

Mr. Chairman, let me remind you that I showed you just such a map in closed session. This array meant that, when the military campaign to topple the Taliban and destroy al-Qa'ida began last October, we were able to support it with an enormous body of information and a large stable of assets.

The realm of human source collection is frequently divided between that which we learned from our foreign partners and unilateral reporting. Even before the plan, our vision for human intelligence on terrorism was simple. We needed to get more from both types. The amounts of both sources of intelligence rose every year after 1998.

And in 1999, for the first time, as I have testified, the volume of reporting on terrorism from our own assets exceeded that from foreign intelligence services, a trend which has continued in subsequent years. The integration of technical and human sources has been key to our understanding of and our actions against international terrorism. It was this combination, this integration, that allowed us years ago to confirm the existence of numerous al-Qa'ida facilities and training camps in Afghanistan.

On a virtual daily basis, analysts and collection officers from NSA, NIMA and CIA came together to interactively employ satellite imagery, communications information, and human source reporting. The integration also supported military targeting operations before September 11, and after, when it helped provide base-

line data for the U.S. Central Command's target planning against al-Qa'ida facilities and infrastructure throughout Afghanistan.

Even while targeting Usama bin Ladin and al-Qa'ida in their Afghan lair, we did not ignore cells of terror spread across the globe. We accelerated our work to disrupt and destroy al-Qa'ida cells wherever we found them. By 1999 the intensive nature of our operations was disrupting elements of bin Ladin's international infrastructure. We went after his leaders and pursued terrorists and other groups engaged in planning future attacks.

By September 11, CIA and, in many cases, with the FBI, had rendered 70 terrorists to justice around the world. Over a period of months, that there was close daily consultation—excuse me. During the Millennium period, we told senior policymakers to expect between 5 and 15 attacks both here and overseas.

The CIA overseas and the FBI in the United States organized an aggressive integrated campaign to disrupt al-Qa'ida's human assets, technical operations and the hand-off of foreign intelligence to facilitate core Foreign Intelligence Surveillance Act warrants. Over a period of months, there was close daily consultation that included the Director of the FBI, the National Security Advisor and the Attorney General.

We identified 36 terrorist agents at this time around the world. We pursued operations against them in 50 countries. Our disruption activities succeeded against 21 of these individuals and included terrorist arrests, renditions, detentions, surveillance and direct approaches. We assisted the Jordanian government in dealing with terrorist cells that planned to attack religious sites and tourist hotels. We helped track down the organizers of these attacks and helped render them to justice.

We mounted disruption and arrest operations against terrorists in eight countries on four continents, which netted information that allows us to track down even more suspected terrorists. During this same period, unrelated to the Millennium threats, we conducted multiple operations in East Asia, leading to the arrest or detention of 45 members of the Hizbollah network.

In December of 1999, an al-Qa'ida operative named Ressam was stopped trying to enter the U.S. from Canada. During the period of the Millennium threats, one of our operations and one of our mistakes occurred during our accelerating efforts against bin Ladin's organizations, when we glimpsed two of the individuals who later became the 9/11 hijackers, Khalid al-Mihdhar and Nawaf al-Hazmi.

In December of 1999, CIA, FBI and the Department of State received intelligence on the travels of suspected al-Qa'ida operatives Nawaf and Khalid to Kuala Lumpur, Malaysia. CIA saw the Kuala Lumpur gathering as a potential source of intelligence about a possible al-Qa'ida attack in Southeast Asia.

We initiated an operation to learn why those suspected terrorists were traveling to Kuala Lumpur. Khalid and Nawaf were among those travelers who, at the time, we knew nothing more about them. We arranged to have them surveilled. It is important to note that the origin of the operation was a piece of information the FBI passed to U.S. intelligence in August of 1998.

Mr. Chairman, there is a more detailed explanation in the formal statement, but let me walk through the facts. On the fourth of January, based on intelligence, FBI headquarters, its New York field office, CIA, our Counterterrorism Center, and stations overseas knew the full name of one of these individuals, Khalid al-Mihdhar, who intelligence told us all was an individual with possible ties to Usama bin Ladin, and the Mujahidin in Yemen, was traveling to Kuala Lumpur.

On the same day, the fourth of January of 2000, CIA obtained a photocopy of al-Mihdhar's passport as he traveled to Kuala Lumpur.

It showed a U.S. multiple-entry visa in Jeddah on 7 April 1999, and expiring on 6 April, 2000. As the operation was under way, CIA briefed senior FBI counterterrorist officers about its progress. CIA continued to keep the FBI apprised of the results of the operation.

On the fifth of January, the CIA officer responsible for initiating and running the operation informed her colleagues at CIA headquarters and abroad in a formal cable that CIA had passed a copy of al-Mihdhar's passport with its U.S. visa to the FBI for further investigation.

I recognize what Ms. Hill said in her opening statement. I can only tell you that I have interviewed this officer. She is a terrific officer. She believes she never would have written this cable unless she believes this had happened. That is as far as we can take that story. It, in no way, absolves us of the responsibility for the watchlisting which I will further on complete.

The suspected terrorists left Kuala Lumpur before we could learn about what they discussed at the meeting. At the time, we did not know enough about them to assess their significance or the threat that they might pose, but we continued to try to learn more.

In March of 2000, a foreign intelligence office told us that Nawaf al-Hazmi had flown to Los Angeles a week after the Kuala Lumpur meeting ended. The service did not know that al-Mihdhar was on the same flight. We did not learn that piece of information until August of 2001.

As the active phase of the Kuala Lumpur operation ended, CIA suspected that al-Mihdhar was a terrorist and knew he had a visa to enter the United States. Those facts met the State Department's standards for adding his name to its watchlist. CIA's lapse in not providing that information to the State Department was caused by a combination of inadequate training of some of our officers, their intense focus on achieving the objectives of the operation itself, determining whether the Kuala Lumpur meeting was a prelude to a terrorist attack and the extraordinary pace of operational activity at the time.

The report that suspected terrorist Nawaf al-Hazmi had traveled to the United States also should have triggered an early effort to notify the State Department and other agencies. However, the information-only message came almost two months after the terrorists left Kuala Lumpur and no CTC officer involved with the operation recalls seeing the message when it arrived at headquarters.

Again, the pace of operations may have been a factor in the missing information. Later in 2000, in the course of supporting FBI's

investigation of the attack on the USS *Cole*, CIA officers looked at the Kuala Lumpur meeting again but in their focus on the investigation did not recognize the implications of the information about al-Hazmi and Mihdhar that they had in their files. During August of——

Chairman GRAHAM. Mr. Tenet, 21 minutes now.

Director TENET. Well, sir, I just have to say, I have been waiting a year. I have got about another 20 minutes. I think I want to put this in the record. It is important. It is contextual, it is factual, and I would like to proceed.

During August of 2001, CIA had been increasingly concerned about a major terrorist attack on U.S. interests, and I directed a review of our files to identify potential threats. In the course of that review, the Counterterrorism Center found that these two individuals had entered the United States.

On August the 23, CIA sent a message marked "immediate" to the Department of State, INS, Customs and FBI, requesting that they be watchlisted immediately. Before August 2001, CIA should have sent the names of both Hazmi and Mihdhar to the State Department for inclusion in its watchlist. The error exposed weaknesses in our internal handling of watchlisting which have been addressed; corrective steps have been taken. The CIA and the State Department are cooperating to transform the TIPOFF all-source watchlist system into a national watchlist center.

The center will serve as a point of contact and coordination for all watchlists in the United States Government. It will also allow us to process more efficiently the increase in terrorism intelligence from intelligence and law enforcement agencies. We have increased the managerial review of the system to reduce the chance that watchlist opportunities will be missed. We have designed a database and assembled a team to consolidate information on the identities of known and suspected terrorists and to flag any that have not been passed to the proper audience.

We have lowered the threshold for nominating individuals for the watchlist and clarified that threshold for our officers. We have lowered the threshold of dissemination of information that used to be closely held as operational.

Returning to the story of what happened in the run-up to 9/11, in the months after the Millennium period, in October of 2000 we launched a serious battle when the USS *Cole* was bombed and 17 brave American sailors perished.

The efforts of American intelligence to strike back at a deadly enemy continued through the Ramadan period in the winter of 2000, another phase of peak threat reporting.

Terrorists cells planning attacks against the United States, foreign military and civilian targets in the Persian Gulf were broken up, capturing hundreds of pounds of explosives and other weapons, including anti-aircraft missiles. We succeeded in bringing a major bin Ladin terrorist facilitator to justice, with the cooperation of two foreign governments. This individual had provided documents and shelter to terrorists traveling throughout the Arabian Peninsula. We worked with numerous European governments such as the Italians, the Germans, the French and the British to identify and

break up terrorist groups and plans against American and local interests in Europe.

Taking the fight to bin Ladin and al-Qa'ida was not just a matter of mobilizing our Counterterrorism Center or even CIA; this was an interagency and international effort. Two things which are critical in this effort are fusion and sharing. The Counterterrorism Center was created to enable the fusion of all sources of information in a single action-oriented unit. Not only do we fuse every source of information or reporting on terrorists, we fuse analysis and operations. This fusion gives us the speed that we must have to seize fleeting opportunities in the shadowy world of terrorism.

Based on this proven philosophy, by 2001 the Center had more than 30 officers from more than a dozen agencies on board, 10 percent of its complement at the time. No matter how it is fused within Counterterrorism Center, no matter how large CTC may be, there are still key counterterrorist players outside of it.

If you interview anyone today in the Counterterrorism Center, he or she will tell you of the work that they are doing with their counterparts across CIA, within NSA, with NIMA, or FBI, or today with a special operations unit in Kandahar or Baghram. It is also clear that when errors occur, when we miss information or opportunities, it is because our sharing and our fusions are not as strong as they need to be.

Communication across bureaucracies, missions and cultures is among our most persistent challenges in the fast-paced, high-pressure environment of counterterrorism, and I will return to this later in my testimony.

One of the most critical alliances in the war against terrorism is that between CIA and FBI. The alliance the last few years has produced achievements that simply would not have been possible if some of the media stories of all-out feuding were true.

An FBI officer has been serving as deputy chief of CTC since the mid-1990s, and FBI reciprocated by making a CIA officer deputy in the Bureau's Counterterrorism division. In the bin Ladin issue station itself, FBI officers were detailed there soon after it opened in 1996.

Of course, this is not a perfect relationship. Frictions often develop. In 1994, a CIA inspector general noted that the interactions between the two organizations were too personality dependent. This has been particularly so when the two were pursuing different missions in the same case, the FBI trying to develop the case for courtroom prosecution, the CIA trying to develop intelligence to assess and counter the threat.

In 2001, before 9/11, the CIA inspector general found significant improvement, citing, for example, the Center's assistance to the FBI in two dozen renditions in 1999 and 2000. The Director of the FBI, Louis Freeh, and I worked hard and together on this. We had quarterly meetings of our senior leadership teams. Through training and other means, coordination between our chiefs of station and our Legats overseas was significantly improved.

Today Bob Mueller and I are working to deepen our cooperation, not only at headquarters but in the field. We both understand that, despite different missions and cultures, we need to build a system of seamless cooperation that is institutionalized.

Mr. Chairman, the third period is the run-up period to 9/11. As with the Millennium and Ramadan 2000 periods, we increased the tempo of our operations against al-Qa'ida. We stopped some attacks and caused terrorists to postpone others.

We helped to break up another terrorist cell in Jordan and seized a large quantity of weapons, including rockets and high explosives. Working with another partner, we broke up a plan to attack U.S. facilities in Yemen.

In June, CIA worked with a Middle East partner to arrest two bin Ladin operatives planning attacks on U.S. facilities in Saudi Arabia. In June and July, CIA launched a wide-ranging disruption effort against bin Ladin's organization with targets in almost two dozens countries.

Our intent was to drive up bin Ladin's security concerns and lead his organization to delay or cancel its attacks. We subsequently received reporting that attacks were delayed, including an attack against the U.S. military in Europe.

In July, a different Middle East partner helped bring about the detention of a terrorist who had been directed to begin an operation to attack an American embassy or cultural center in a European capitol.

In the summer of 2001, local authorities, acting on our information, arrested an operative described as bin Ladin's man in East Asia. We assisted another foreign partner in the rendition of a senior bin Ladin associate. Information he provided included plans to kidnap Americans in three countries and carry out hijackings.

We provided intelligence to a Latin American service on a band of terrorists considering hijackings and bombings. An FBI team detected explosives residue in their hotel rooms. In the months leading up to 9/11, we were convinced that bin Ladin meant to attack Americans, meant to kill in large numbers, and that the attack could be at home, abroad, or both. And we reported these threats urgently.

Our collection sources lit up during this intense period. They indicated that multiple spectacular attacks were planned and that some of these plots were in the final stages. Some of the reporting implicated known al-Qa'ida operatives. The report suggested that the targets were American, although some reporting simply pointed to the West or to Israel.

But the reporting was maddeningly short on actionable details. The most ominous reporting hinting at something large was also most vague. The only occasions in this reporting where there was specific geographic context, either explicit or implicit, it appeared to point abroad, especially to the Middle East.

We disseminated these raw reports immediately and widely to policymakers and action agencies such as the military, the State Department, the FAA, the FBI, and others. The reporting by itself stood as a dramatic warning of imminent attack. Our analysts worked to find linkages among the reports as well as links to past terrorist threats and tactics.

We considered whether al-Qa'ida was feeding us this reporting, trying to create panic through disinformation. Yet we concluded that the plots were real. When some reporting hinted that an at-

tack had been delayed, we continued to stress that there were indeed multiple attacks planned and that several continued on track.

And when we grew concerned that so much of the evidence pointed to attacks overseas, we noted that bin Ladin's principal ambition had long been to strike the United States. Nevertheless, with regard to the 9/11 plot, we never acquired the level of detail that allowed us to translate our strategic concerns into something that we could act on.

The Intelligence Community Counterterrorism Board issued several reports that summer. A sign that our warnings were being heard, both from our analysis and from the raw intelligence we disseminated was that the FAA issued two alerts to air carriers in the summer of 2001.

Our warnings complemented strategic warnings that we have been delivering for years about the real threat of terrorism to America. There is no need to go through it, but you know, Mr. Chairman, in three separate occasions in my worldwide threats testimony, I told you that, as I told you in 1999, there is not the slightest doubt that Usama bin Ladin, his worldwide allies and his sympathizers are planning further attacks against us.

I told you that he will strike whenever in the world he thinks we are vulnerable and that we were concerned that one or more of bin Ladin's attacks could occur at any time. In 2001 I told you that the terrorists are seeking off softer targets that provide opportunities for mass casualties and that bin Ladin is capable of planning multiple attacks with little or no warning.

I looked at the strategic warnings that had been issued on hijacked aircraft. Early in the 1990s, we had some serious strategic analytic work on both terrorist targets and methodology. The National Intelligence estimate in 1995 warned: The United States is particularly vulnerable to various types of terrorist attacks. Several kinds of targets are especially at risk—national symbols such as the White House, the Capitol, and symbols of U.S. capitalism, such as Wall Street, power grids, communication switches, particularly civil aviation.

The same estimate also said we also assess that civil aviation will figure prominently among possible terrorist targets in the U.S. This stems from the increase in domestic threat posed by the foreign terrorists, the continued appeal of civil aviation as a target, and a domestic aviation security system that has been the focus of media attention.

We have evidence that individuals linked to terrorist groups or state sponsors have attempted to penetrate security at U.S. airports in recent years. The media have called attention to, among other things, inadequate security for checked baggage.

A review of the evidence obtained thus far about the plot uncovered in Manila in early 1995 suggests that conspirators were guided in their selection of the method and venue of attack by carefully studying security procedures in place in the region. Terrorists operating in this country are similarly methodical; they will identify serious vulnerabilities of our security system of domestic flights.

In a 1997 update we said pretty much the same thing. It is clear that the message was received. The White House Commission on

Aviation Safety and Security noted a number of facts consistent with this in their report which you have in the record.

It its publication Criminal Acts Against Civil Aviation, the FAA stated that although bin Ladin is not known to have attacked civil aviation, he has both the motivation and the wherewithal to do so. Bin Ladin's anti-western and anti-American attitudes make him and his followers a significant threat to civil aviation, especially U.S. civil aviation. We have given you over a half a million pages of documents and interviewed hundreds of intelligence officers in their efforts to investigate this complex issue.

The documents we provided show some 12 reports spread over seven years which pertain to possible use of aircraft as terrorist weapons. We disseminated those reports to the appropriate agencies such as the FAA, the Department of Transportation, and the FBI as they came in. Moreover, we also provided versions of intelligence reports that were about threats to civil aviation so they could be distributed more widely through the airline industry.

Mr. Chairman, I want to talk about two more subjects—and I appreciate the fact that you are letting me go on—budget and resources. Mrs. Pelosi, you were right; no one should hide behind budget and resources as an excuse for anything. But there is a context to budget and resources that is important for us to evaluate.

To evaluate our work, it is essential that you look at three issues: Global geopolitical issues we were grappling with; counterterrorism resource changes throughout the 1990s that affected our ability to fight; and the overall health of U.S. intelligence during this period. It is simply not enough to look at al-Qa'ida in isolation.

The last decade saw a number of conflicting and competing trends—military forces deployed to more locations than ever in our country's history, the growing counterproliferation in counterterrorism threat, constant tensions in the Middle East, and to deal with these and a host of other issues, far fewer intelligence dollars and manpower.

At the end of the Cold War, the Intelligence Community, with a $300 billion deficit and budget caps much like the rest of the National Security Community, was asked by both Congress and successive administrations to pay the peace dividend. The cost of the dividend was that during the 1990s the Intelligence Community funding declined in real terms, reducing our buying power by tens of billions of dollars over the decade.

This loss of people was devastating, particularly in our two most manpower-intensive activities, all-source analysis and human source collection. By the mid 1990s, recruitment of CIA analysts and case officers had come to a virtual halt.

NSA was hiring no new technologists during the greatest information technology change in our lifetime. During this period, it was the exception that we would surge—our expectation that we would surge our existing resources to deal with emerging intelligence challenges, including threats from terrorism, and surge we did.

As I declared war on al-Qa'ida in 1998 in the aftermath of the East Africa bombings, we were in the fifth year of around-the-clock support to Operation Southern Watch. Just three months earlier,

we were embroiled in answering questions on the India-Pakistan nuclear tests and trying to determine how we could surge more people to understanding and countering weapons of mass destruction.

In early 1999, we surged more than 800 analysts and redirected collection assets to support the NATO bombing campaign against the Federal Republic of Yugoslavia.

During this time period of increased military operations, the Defense Department was also reducing its tactical intelligence units and funding. This caused the Intelligence Community to stretch our capabilities because national systems were covering the gaps in tactical intelligence. While we grappled with this multitude of high priority and overlapping high crisis, we had no choice but to modernize selective intelligence systems and infrastructure in which we deferred necessary investments while we downsized or we would have found ourselves out of business.

We had a vivid example of the cost of deferring investments a few years ago when NSA lost all communications between the headquarters and its field stations and were unable to process that information for several days. Throughout the Intelligence Community, during this period, we made difficult resource allocation decisions to try to rebuild critical mission areas.

In CIA was launched a program to rebuild our clandestine service. This meant overhauling our recruitment and training practices and our infrastructure. We launched similar initiatives to rebuild our analytical depth and expertise and to reacquire the cutting edge in technology. Although we will not be given credit for these efforts in the war on terrorism, that most assuredly contributed to that effort.

NSA made the hard decision to cut additional positions to free up pay and benefit dollars to patch critical infrastructure problems and to modestly attempt to capitalize on the technology revolution.

But, with the al-Qa'ida threat growing more ominous and with our resources devoted to countering the threat clearly inadequate, we began taking more money and people away from other critical areas to improve our efforts against terrorism. We managed to triple the Intelligence Community-wide funding for counterterrorism from the period of 1990 to 1999.

The Counterterrorism Center's resources nearly quadrupled in the same period. As your own joint inquiry charts show, we had significantly reallocated both dollars and people inside our programs to work the terrorism problem.

Inside CIA, the 1990s reflect the same pattern. CIA's budget had declined 18 percent, we had lost 16 percent of our personnel. Yet in the midst of this stark resource picture, our funding level for counterterrorism just prior to 9/11 was 50 percent higher than our 1997 level.

CTC personnel increased by over 60 percent during the same period. The CIA consistently reallocated and sought additional resources in this fight. In 1994, the budget request for counterterrorism equaled less than four percent of our program total. In the fiscal 2002 budget request we submitted prior to 9/11, counterterrorism activities constituted almost 10 percent of the budget increase.

During a period of budget stringency when we were faced with rebuilding essential intelligence capabilities, I made some tough choices. Although resources for virtually everything else at CIA was going down, counterterrorism resources went up.

After the U.S. embassies in Africa were bombed, we requested more money. In the fall of 1998, I asked the administration to increase intelligence funding by more than $2 billion annually for the fiscal years 2000 to 2005. And each subsequent FYDP program I made similar requests. Only small portions of these requests were approved.

Counterterrorism funding and manpower needs were number one in every list that I provided to the Congress and the administration. Indeed, it was at the top of the funding list approved by Speaker Gingrich in 1999, the first year in which we received a significant infusion of new money for intelligence.

That supplemental and those that follow it that you supplied were essential to our efforts, and they helped save American lives. We knew we could not count on supplementals to build multi-year programs. That is why we have worked so hard to reallocate our resources and seek five-year funding increases. Many of you on this committee and the appropriations committees understood the problem very well. You were enormously helpful to us and we are grateful.

I want to conclude on the resource point by saying one thing. In CIA alone, I counted the equivalent of over 700 officers working counterterrorism in August of 2001, at both headquarters and in the field. The number does not include the people who are working to penetrate, either technically or through human sources, a multitude of terrorist targets which we could drive intelligence on terrorists, nor does it include friendly liaison services, or coalition partners.

You simply cannot gauge the level of effort by counting only people who had the words "al-Qa'ida" or "bin Ladin" in their position description. We reallocated all of the people we could, and we always knew that we never had enough. We can argue for the rest of the day about the exact number of people we had working this problem, but we never said that the numbers we had were enough. Our officers told your investigators that they were always shorthanded. They were right. They were.

America may never know the names of those officers. But America should know they are heros. They worked tirelessly for years to combat bin Ladin and al-Qa'ida and have responded to the challenge of combating terrorism all during this time with remarkable intensity. Their dedication, professionalism and creativity stopped many al-Qa'ida plots in their tracks and saved countless American lives. Most of them are still in this fight, are essential to this fight, and they honor all of us by their continued service.

Let me close with some points, Mr. Chairman. Success against terrorist targets must be measured against all elements of our Nation's capabilities, policies, and will. The Intelligence Community and the FBI are important parts of the equation, but by no means the only parts. We need a national integrated strategy in our fight against terrorism that incorporates both offense and defense. The strategy must be based on three pillars: Continued relentless effort

to penetrate terrorist groups, whether by human or technical means, whether alone or in partnership with others.

Intelligence, military law enforcement and diplomacy must stay on the fence continually against terrorism around the world. We must disrupt and destroy the terrorist operational chain of command, and the momentum to deny them sanctuary anywhere and eliminate their sources of financial and logistical support.

Nothing did more for our ability to combat terrorism than the President's decision to send us into the terrorist sanctuary. By going in massively, we were able to change the rules for the terrorist. Now they are the hunted. Now they have to spend their time worrying about their survival. Al-Qa'ida must never again acquire a sanctuary anywhere.

On defense, we need systematic security improvements to protect our country's people and our infrastructure and create a more difficult operating environment here in the United States for terrorists. The objective is to understand our vulnerabilities better than the terrorists do, to take actions to reduce the vulnerabilities, to increase the costs and risks for terrorists to operate in the United States and, over time, to make those costs unacceptable to them.

We have learned an important historic lesson. We can no longer race from threat to threat, resolve it, disrupt it, and then move on. Targets at risk remain at risk. In 1993, the first attack on the World Trade Center was damaging, maybe modestly so compared, but very damaging. A plot around the same time to attack New York City tunnels and landmarks was broken up. We all breathed a sigh of relief and moved on, focusing the effort mostly on bringing the perpetrators to justice. The terrorists came back.

At the Millennium, a young terrorist panicked at a Canadian-U.S. border crossing, and his plan to attack an airport in Los Angeles was exposed and thwarted. We breathed another sigh of relief and prepared for his trial. Al-Qa'ida's plans had only been delayed.

Last winter, another young terrorist on an airliner ineptly tried to detonate explosives in his shoes and was stopped by alert crew and passengers. At this point we are smarter. We started checking people's shoes for explosives. It is not nearly enough. In the last year, we have gone on high alert several times for good reason, only to have no attack occur.

We all breathed a sigh of relief and thought maybe it was a false alarm. It wasn't. We must design systems that reduce both the chances of an attack getting through and the impact if it does. We must address both the threat and our vulnerability; we must not allow ourselves mentally to move on while the enemy is still at large.

Two final points. Our people need better ways to communicate. Moreover, we also need systems that enable us to share critical information quickly across bureaucratic boundaries—systems to put our intelligence in front of those who need it wherever they may be, whatever their specific responsibilities for protecting the American people from the threat of terrorist attack. This means we must move information in ways and to places it never had to move before.

We are improving our collaborative systems. We need to improve our multiple communications links, both within the Intelligence

Community and now to homeland security. Now, more than ever before, we need to make sure our customers get from us exactly what they need, which generally means exactly what they want, fast and free of unnecessary restrictions.

Chiefs of police across the country express understandable frustration at what they do not know. But there is something else. Intelligence officers in the Federal Government want to get their hands on locally-collected data. Each could often use what the other may have already collected. The proposed Department of Homeland Security will help. So too will the Intelligence Community's experience in supporting our Armed Forces. We are going to have to put that experience to work in supporting the police chiefs. We don't have the luxury of an alternative.

This fight is going to be long and difficult. It will require the patience and the diligence that the President has asked for. It will require resources sustained over a multi-year period to recapitalize our intelligence infrastructure on a pace that matches the changing technical and operational environment that we face. It will also require countries that have previously ignored the problem of terrorism or refused to cooperate with us to step up and choose sides.

It will require all of us across the government to follow the example of the American people after September 11 to come together, to work as a team, and pursue our mission with unyielding dedication and unrelenting fidelity to our highest ideals. We owe those who died on September 11 and all Americans no less.

Chairman GRAHAM. Thank you, Mr. Director.

Director Mueller.

[The prepared statement of Mr. Mueller follows:]

TESTIMONY OF
ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION
BEFORE THE
SENATE SELECT COMMITTEE ON INTELLIGENCE
AND THE
HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

OCTOBER 17, 2002

Chairman Graham, Chairman Goss, Senator Shelby, Congresswoman Pelosi and Members of the Committees. Thank you for the opportunity to appear before you this morning to discuss the events of September 11, 2001 and the FBI's counterterrorism efforts since that tragic day. Before addressing these matters, I would like to take a moment to honor the victims who died at the hands of Al Qaeda terrorists. We cannot begin to imagine how difficult this past year has been for the families. There can be little doubt that the pain, the anger, and the grief is as fresh today as it was on that Tuesday morning last year. Families have lost mothers, fathers, daughters and sons -- the public safety community has lost courageous firefighters and law enforcement officers -- all of them, innocent people going about their daily lives. We in the FBI extend our deepest sympathy to the surviving family members and victims of these attacks and to assure them that the FBI is determined to honor the memory of their loved ones by never wavering in our fight against terrorism.

Mr. Chairman, I would also like to take a moment to recognize and thank a number of people for their exceptional support.

First, I would like to express my deep and abiding gratitude to Director Tenet and General Hayden for their leadership as we work together to confront the challenges before us. As I have stated many times since September 11th, the terrorist threat is far too great for any one agency to address on its own. We must all work together -- at the federal, state, local, and international level -- to successfully combat terrorism.

Louis Freeh, my predecessor as Director of the FBI, who appeared before this Committee last week, gave a thoughtful, historical perspective about his efforts during the 1990s to combat terrorism at home and abroad. He is owed a debt of gratitude for his service as an FBI Agent, a federal prosecutor, a U.S. District Court Judge, and as FBI Director.

I would also like to acknowledge the superb team of FBI employees who provided extraordinary support to this Committee for the past six months. As you know, members of your staff took up permanent residency at FBI Headquarters on April 1, 2002. Since then, we have

assigned 20 of our best analysts, Agents, and lawyers, who have worked night and day to accommodate this Committee's requests. These employees have provided your staff with secure workspace, equipment, clearances and other logistical provisions; they have identified, located and processed for release to the Committee over 24,000 pages of sensitive documents; and they have arranged for Committee staff to conduct over 150 interviews of FBI employees across the country and in our Legal Attache offices around the world. The FBI's cooperation with this inquiry has been extensive.

Finally, and most importantly, I would like to recognize the men and women of the FBI, particularly those serving as analysts and agents in the counterterrorism program. These are dedicated, hardworking, and underappreciated public servants who were devastated by the events of 9/11. These men and women have struggled day in and day out to do their jobs despite inadequate resources and enormous workloads. I have been honored to work alongside these employees -- and all the men and women of the FBI -- for the past year. Their unrelenting perseverance and their unassuming heroism have truly been an inspiration.

I. HISTORY OF THE TERRORIST THREAT

I believe it is important to remind this Committee and the American people that the mission of the FBI's counterterrorism program -- to identify, prevent, deter and respond to acts of terrorism -- is broad and multi-faceted. While the events of 9/11 have brought into focus the threat posed by Usama Bin Laden and the Al Qaeda network, we must recognize that the threats we face are not limited to one individual, one group, or one country. Our counterterrorism efforts must address the threats posed by a multitude of international and domestic terrorists.

Our recent history reflects growing threats from a variety of groups and individuals. Loosely affiliated religious extremists committed the bombings of the World Trade Center in 1993; Khobar Towers in 1996; the Embassies in Kenya and Tanzania in 1998 and the *U.S.S. Cole* in October 2000. More structured terrorist organizations were responsible for numerous other terrorist attacks. Hizballah, for example, killed more Americans prior to 9/11 than any other terrorist group, including Al Qaeda, with their 1983 truck bombings of the U.S. Embassy and U.S. Marine Corps barracks in Lebanon, the 1984 bombing of the U.S. Embassy Annex in Beirut, and the 1985 hijacking of TWA Flight 847. Also, right-wing terrorist groups espousing principles of racial supremacy and anti-government rhetoric have become a serious menace, as tragically evidenced by the April 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City.

At the same time, the FBI and our partners have prevented significant terrorist acts: the 1993 plot to bomb New York landmarks; the 1995 plans to bomb U.S. commercial aircraft transiting the Far East; the 1997 plot to place four pipe bombs on New York City subway cars which was narrowly averted by the New York Joint Terrorist Task Force; the 1997 prevention of possible detonation of 10 letters bombs at Leavenworth Federal Prison and two offices of the al-

Hayat newspaper; and the 1999 investigation, in coordination with the U.S. Customs Service, which resulted in the conviction of Ahmed Ressam for a plot to bomb Los Angeles International Airport at the turn of the millennium.

In addition to the terrorist activities of these individuals and groups, the FBI is confronting a growing interest in the acquisition of weapons of mass destruction by terrorists and other groups. Given the potential for inflicting large-scale injury or death, the efforts of international and domestic terrorists to acquire weapons of mass destruction have been a significant and growing concern for the FBI. Prior to September 11, 2001, the number of weapons of mass destruction -- or "WMD" -- cases initiated for 2001 was 100, of which 67 were biological. Since 9/11 and the anthrax attacks of last fall, the FBI has responded to approximately 7,089 suspected anthrax letters, 950 incidents involving other potential weapons of mass destruction -- such as bomb threats -- and an estimated 29,331 telephone calls from the public about suspicious packages.

In the 1990s, terrorist groups started using new information technology and the Internet to formulate plans, recruit members, communicate between cells and members, raise funds, and spread propaganda. Their aptitude with this technology facilitates their terrorism preparation and operations and raises the specter that they will use their cyber-tools against our critical infrastructures.

In response to these disturbing trends, Director Freeh designated Counterterrorism a Tier One priority in May 1998, and he began focusing additional attention and resources on the program. By late 1999, the FBI's Senior Executive Managers had formulated and were implementing an initiative designed to position the FBI to be at its maximum capacity to address the Counterterrorism threat by the year 2005. As Dale Watson, Executive Assistant Director for Counterterrorism testified before this Committee, the initiative was still underway on September 11, 2001.

II. THE SEPTEMBER 11th INVESTIGATION

Immediately after the September 11th attacks, the FBI, the law enforcement community and the U.S. and Foreign Intelligence Communities joined forces to find out everything we could about the hijackers and how they succeeded. Our immediate goal was simple -- to prevent another attack by fully understanding how the terrorists perpetrated this one.

The FBI's contribution to this effort has been significant. Thousands of FBI Agents from each of our 56 field offices have participated in the investigation; agents have covered over 337,000 leads and have produced more than 165,000 FD-302 reports of investigation; nearly 300 Special Agents and 85 Support employees have been detailed to more than 30 Legal Attache offices overseas to assist in pursuing leads and coordinating the investigation with our international colleagues; and to date, the FBI Laboratory has received over 660 submissions of

evidence from the crash sites and related searches, representing approximately 7,332 items of potential evidence.

Thanks to these efforts and the unprecedented cooperation of the intelligence and law enforcement communities -- both domestic and international -- our investigation has revealed many of the details about the planning, financing and perpetration of these attacks. While our investigation continues and will likely develop new and significant details for years to come, let me summarize the findings presented in my testimony before this Committee in June.

- Each of the hijackers, apparently selected to avoid notice, came easily and lawfully from abroad under valid visas: fifteen were Saudi Arabia nationals, two were United Arab Emirates (UAE) nationals, and one each were from Lebanon and Egypt.

- The plot for the September 11th attacks was conceived in Afghanistan, with details developed and coordinated in Hamburg, Germany.

- The hijackers entered the United States through 8 different cities over a period of 19 months. They each entered the country lawfully and had valid visas at the time of the attacks.

- While in the United States, the hijackers effectively operated without suspicion, triggering nothing that alerted law enforcement. They committed no crimes with the exception of minor traffic violations. They dressed and acted like Americans, shopping and eating at places like Wal-Mart and Pizza Hut.

- They relocated frequently and did not hold jobs. When three got speeding tickets in the days leading up to September 11, they remained calm and aroused no suspicion.

- None of the nineteen suicide hijackers is known to have had computers, laptops, or storage media of any kind, although they are known to have used publicly accessible Internet connections at various locations. They used 133 different pre-paid calling cards to call from various pay phones, cell phones, and land lines.

- The nineteen suicide hijackers used U.S. checking accounts accessed with debit cards to conduct the majority of financial activity during the course of this conspiracy.

- The hijackers conducted meetings and communications without detection, took apparent surveillance flights, and passed through airport security screening without notice.

- In August, the hijackers purchased tickets for the September 11th flights either in cash directly at the ticket counters or using the Internet.

- In the weeks immediately preceding September 11th, the hijackers moved into position, gathering in East Coast cities in Massachusetts, Maryland and New Jersey.

- They boarded cross-country flights in the early hours of September 11th, doing nothing that would arouse suspicion.

I believe that the context in which these 19 individuals were able to come to the United States, take advantage of the liberties this country has to offer, and operate without detection is important to a full understanding of how these attacks were perpetrated.

III. FBI's POST-9/11 INVESTIGATIVE ACTIVITY

In addition to investigating the 9/11 attacks, the FBI and our partners have undertaken investigations and operations over the last year that have dealt blows to a number of terrorist groups.

- Two weeks ago, the Joint Terrorism Task Forces in the Portland, Oregon office and the Detroit, Michigan office arrested four individuals on charges of aiding, and in some cases, trying to join Al Qaeda fighters. Two other individuals were charged, one of whom recently turned himself into Pakistani authorities. The other remains a fugitive. The indictment alleges that all six members of this group conspired to travel to Afghanistan to join Al Qaeda and Taliban forces in the jihad and to take up arms against U.S. and allied military forces.

- Last month, the Buffalo, New York Joint Terrorism Task Force executed search warrants on properties located in Lackawanna, New York and arrested individuals who had traveled overseas in the Summer of 2001 to attend the al-Farooq terrorist training camp located near Kandahar, Afghanistan. During their stay at the camp, these individuals received terrorism training and a speech from Usama bin Laden.

- In May, the FBI served a material witness warrant on a U.S. citizen, Abdullah Al Muhajir, also known as Jose Padilla, as he entered the United States from Pakistan at Chicago's O'Hare International Airport. Soon thereafter, Padilla was transferred to the custody of the Defense Department where he is being detained as an "enemy combatant."

- Last week in Chicago, the Executive Director of Benevolence International Foundation (BIF), a purportedly charitable organization, was charged in a racketeering conspiracy to fraudulently raise funds for Al Qaeda and other violent

groups, as part of a multi-national criminal enterprise over a 10-year period. The FBI's Terrorist Financial Operations Section conducted the financial investigation of BIF, in addition to 40 other major counterterrorism cases. Although the details of these investigations remain classified, they have denied Al Qaeda millions of dollars in financing.

- As a result of U.S. military and intelligence community action in Afghanistan, Pakistan and other foreign lands, a large volume of paper documents, electronic media, videotapes, audiotapes and electronic equipment has been seized. The FBI, CIA, DIA and NSA have established a coordinated effort to exploit these seized materials. The Document Exploitation project identifies and disseminates pieces of intelligence gleaned from its review of these materials.

These are just a sampling of the investigative and preventive efforts that have born fruit over the last year. There are others, but those operations remain classified and have been described in closed sessions with the Members of this Committee.

IV. FBI's POST-9/11 REFORMS

The 13 months since the September 11th attacks have been a time of great change for the Federal Bureau of Investigation. Starting immediately after the planes hit, when over half of our 11,500 agents suddenly found themselves working terrorism matters, it became clear that our mission and our priorities had to change. Today, the FBI has twice the number of Agents permanently assigned to counterterrorism as were assigned prior to 9/11. Other permanent changes have been carefully considered and implemented.

Virtually every morning since September 11th, Director Tenet and I brief the President, updating him on the investigation and our response to the various threats we are receiving worldwide. The President wants to know what the FBI is doing -- along with the CIA and our other partners -- to protect Americans against terrorism. That is his bottom line, and it is the touchstone of our efforts to refocus the FBI.

We have been addressing the shortcomings of the Bureau and the Intelligence Community that were highlighted by the September 11th attacks. We have heard, and we acknowledge, the valid criticisms, many of which have been reiterated by this Committee. For example, the Phoenix memo should have been disseminated to all field offices and to our sister agencies; and the 26-page request from Minneapolis for a FISA warrant should have been reviewed by attorneys handling the request. These incidents have informed us on needed changes, particularly the need to improve accountability, analytic capacity and resources, information sharing, and technology, to name a few. We have taken steps to address those shortcomings, some of which I would like to highlight today.

Reorganization of the Counterterrorism Division

In November of last year, Congress approved my proposal for a reorganization of FBI Headquarters. Under this reorganization, the Assistant Director for Counterterrorism is responsible for management of the national terrorism program and for select cases and operations which require national-level management due to special circumstances, situations, or sensitivity. This management structure is a recognition that counterterrorism has national and international dimensions that transcend field office territorial borders and require centralized coordination to ensure that the individual pieces of an investigation can be assembled into a coherent picture

This ensures accountability for the program. Under the prior system -- whereby field offices, and particularly the New York Field Office, would have primary responsibility for terrorism cases -- responsibility was diffused and Bureau leadership could not easily be held accountable for the program. Under the reorganization, the Assistant Director for Counterterrorism is accountable for taking all steps necessary to maximize our counterterrorism capacity.

One of the ways in which Headquarters supports the field in maximizing their counterterrorism capabilities is through the newly created "flying squads." These squads augment local field investigative capabilities with specialized personnel and support FBI Rapid Deployment Teams, thereby providing a surge capacity for quickly responding to fast-breaking situations in locations where there is no FBI presence.

Analytical Enhancements

This Committee is familiar with the FBI's analytical shortcomings, as demonstrated by the limited dissemination and analysis afforded the Phoenix memo. Over the last year, we have undertaken the following measures to enhance our analytical capacity:

- We have created the Office of Intelligence, which is the component of the FBI that will oversee development of the analyst position and career track, and will ensure that intelligence is shared as appropriate within the FBI and the rest of the United States Government. I am grateful to Director Tenet for his willingness to detail experienced CIA managers from the Directorate of Intelligence to the FBI to set up and manage our Office of Intelligence.

- We have significantly increased the resources allocated to analysis. With regard to Intelligence Operations Specialists (IOSs), who provide direct support to investigations, we are proposing a total staffing level of 205, with 89 currently on board and 44 in various stages of the background investigation process. With regard to Intelligence Research Specialists (IRSs), who provide strategic analysis, we are proposing a total staffing level of 155, with 70 currently on board and 73 in the background investigation process.

The FBI has requested an additional 28 IOSs and 114 IRSs in its 2003 budget. I am concerned that until the 2003 budget is approved, the FBI will be held to current spending levels. A long term Continuing Resolution could have a significant impact on our analytical program.

- We have created a College of Analytical Studies (CAS) to provide training for all FBI analytical support personnel. The CAS is intended to become a featured component of training at the FBI Academy, along with New Agents Training and the FBI National Academy.

- Through the efforts of our expanded Terrorist Financial Review Group and the interagency teams conducting document exploitation, we have augmented FBI capabilities to perform financial and communications analyses of terrorist groups and networks.

Information Sharing Enhancements

Much has been made of the reportedly hostile relationship and turf battles between the FBI and the CIA. As you have heard from Director Tenet, the relationship between the FBI and the CIA has never been stronger or more productive. While we concede that there were isolated failings in the information flow between the two agencies prior to 9/11, we must not overlook the fact that a successful, systematic effort has been underway for years to develop and build upon our agencies' relationship.

Starting with Dale Watson's detail to the CIA's Counterterrorism Center in 1996, we have had a regular exchange of employees. At this time, we have 11 employees assigned to the CIA's Counterterrorism Center and the CIA has eight managers and dozens of analysts assigned to the FBI's Counterterrorism Division. Each of these employees has unfettered access to the computer databases and communications systems of the other agency. Every morning, a CIA official detailed to the FBI joins other FBI executives in my office for the twice daily briefing sessions. I rely on his counsel as much as I rely on my own executives. Also, I meet with George Tenet every morning when we brief the President, and I have nothing but the greatest respect for him and his agency.

This Committee has presented select testimony that is critical of the FBI's historical unwillingness and technological inability to share information with not only the CIA but with other federal agencies, and with our state and local law enforcement colleagues. Since 9/11, I have instituted several changes which have resulted in significant improvements in communication and coordination of many aspects of information sharing. I would like to summarize some of the initiatives the FBI has adopted in this regard since 9/11.

- We established Joint Terrorism Task Forces in each of our 56 field offices. Prior to 9/11, only 35 offices had JTTFs. The partnering of FBI personnel with investigators from various local, state and federal agencies on these task forces

encourages the timely sharing of intelligence that is absolutely critical to our counterterrorism mission.

- We established a new National Joint Terrorism Task Force at FBI Headquarters to complement task forces established in each of the FBI's 56 field offices and to improve collaboration and information sharing with other agencies. We currently have representation of 26 federal agencies and two state and local law enforcement officials who report to the FBI's Command Center as part of this initiative.

- We have undertaken the Joint Terrorism Task Force Information Sharing Initiative (JTTF ISI) involving the St. Louis, San Diego, Seattle, Portland, Norfolk and Baltimore field offices. This pilot project, which was first initiated in the St. Louis office, will integrate extremely flexible search tools that will permit investigators and analysts to perform searches on the "full text" of investigative files -- not just indices. An analyst or investigator will be able to smoothly transition from searching text, to reviewing results, to examining source documents, to developing link diagrams, to generating map displays. To insure proper security, four graduated levels of security access are being built into the system.

- We created the Office of Law Enforcement Coordination (OLEC) to enhance the ability of the FBI to forge cooperative and substantive relationships with all of our state and local law enforcement counterparts. The OLEC, which is run by a former Police Chief, also has liaison responsibilities with the White House Office of Homeland Security.

- We established the FBI Intelligence Bulletin which is disseminated weekly to over 17,000 law enforcement agencies and to 60 federal agencies. The bulletin provides information about terrorism issues and threats to patrol officers and other local law enforcement personnel who have direct daily contacts with the general public, contacts which could result in the discovery of critical information about those issues and threats.

As a result of these initiatives, the FBI has received numerous letters of support and gratitude from state and local officials and from the International Association of Chief of Police. I would like to submit some of those letters to the Committee and ask that they be included as part of the official record of this inquiry.

These initiatives represent the priority and emphasis that the FBI leadership and I have put on our commitment to share information and data with other federal agencies, with our state and local law enforcement partners, and amongst ourselves. The institutional change reflected by these initiatives has produced -- and will continue to produce -- measurable progress in the coordination and integration of law enforcement efforts at all levels of government.

Technology

We are also addressing the shortcomings of the Bureau's information technology. Over the years, we have failed to develop a sufficient capacity to collect, store, search, retrieve, analyze and share information. Prior testimony before this Committee has described the problems the FBI is experiencing because of outdated technology. Thanks to support from Congress, the FBI has embarked on a comprehensive overhaul and revitalization of our information technology infrastructure. That process is well under way, but I want to caution you that these problems will not be fixed overnight. Our technological problems are complex, and they will be remedied only through careful and methodical planning and implementation. We have made progress in the past year, and we have laid the groundwork for significant progress in the months and years ahead.

The first major step in the right direction is our Trilogy Program. The Trilogy Program was designed as a 36-month effort to enhance our effectiveness through technologies that facilitate better organization, access and analysis of information. The overall direction of the Trilogy Program is to provide all FBI offices with improved network communications, a common and current set of office automation tools, and easy-to-use, re-engineered, web-based applications.

Under the FBI's old legacy investigative information system, the Automated Case Support (ACS), users navigate with the function keys instead of the point and click method common to web based applications. Simple tasks, such as storing an electronic version of a document today, require a user to perform twelve separate functions, in a "green screen" environment. That will soon change with Trilogy. Automated workflow will allow for a streamlined process to complete tasking. Storing a document for the record will occur with a click of the mouse button. This will make investigative and intelligence information immediately available to all personnel with appropriate security.

Multimedia functionality will allow for the storage of information in its original form. Under the old system, agents cannot store non-compatible forms of digital evidence in an electronic format, and instead have to describe the evidence and indicate where the evidence is stored in a control room. Multimedia functionality will facilitate electronic storage of digital evidence and media to the investigative case file, allowing access to the information from the desktop.

The original plan for Trilogy was development and deployment over 36 months from the date of the contract awards for the infrastructure and applications development, May and June 2001, respectively. The events of September 11, 2001 impacted many aspects of the FBI, including the Trilogy Program. Recognizing the urgent need for improved information technologies, I ordered that Trilogy implementation be accelerated, with emphasis on those capabilities most urgently needed to support the FBI's priority cases. In response, Congress provided additional funding, and Trilogy's network and desktop infrastructure improvements were accelerated. The resulting improvements are significant.

Infrastructure enhancements are being deployed in two phases. The first phase, called "Fast Track", entails installation of Trilogy architecture at our 56 Field Office locations and as many of our Resident Agencies as can be completed before the second phase begins. This architecture includes new network printers, color scanners, local area network upgrades, desktop workstations, and Microsoft Office applications. By the end of April 2002, deployment at all 56 FBI Field Offices and two Information Technology Centers (ITCs) was completed. Fast Track is continuing to deploy this infrastructure to our Resident Agencies.

The second phase of infrastructure deployment is called "Full Site Capability," representing the complete infrastructure upgrade. The full upgrade will provide wide area network connectivity, new encryption devices to protect our data, new operating systems and servers, and new and improved e-mail capability. Completion of this phase was moved from the accelerated date of July 2002 to March 2003 to allow additional time to test and deploy a secure, operational system.

We also recognize that we have a critical need to share Top Secret and Sensitive Compartmented Information (TS/SCI.) data internally, primarily among analysts. We are planning a phased implementation at FBI Headquarters followed by deployment within the Intelligence Community of a system that will markedly increase our ability to conduct strategic analysis.

Once we catch up to a standard PC environment, the future looks very positive. We are planning for a technology refreshment program (TRP) which will incorporate our technology as it becomes available and will replace Trilogy network and workstation hardware, network data storage, server hardware, and embedded software on a periodic basis to prevent system performance degradation. A viable infrastructure technology refreshment plan is essential to maintain the benefits of the Trilogy investment and the efficiency and capabilities of FBI investigative support systems and to better plan and budget for out year expenditures.

IV. CONCLUSION

In the aftermath of the September 11th attacks, the FBI quickly recognized that the organization needed to change in order to address the terrorist threat facing this nation. As I have indicated, the FBI has faced many challenges over the past 13 months and has made significant progress in addressing these challenges. I am proud of the flexibility and the willingness of the FBI workforce to do whatever it takes -- to change whatever needs changing -- to prevent another terrorist attack.

Despite our accomplishments and the success of the FBI reorganization in addressing our shortcomings, however, our transformation must continue. We cannot grow complacent. The FBI must develop a workforce that possesses specialized skills and backgrounds, that is equipped with the proper investigative, technical, and analytical tools, and possesses the managerial and administrative competencies necessary to deal with a complex and volatile environment. To

assist in these efforts, the FBI is in the midst of an internal re-engineering review to examine virtually every aspect of FBI operations, administration, policy and procedure. As a result of this review, we anticipate additional changes to FBI programs that will enable us to most effectively and efficiently utilize the tools and the resources Congress has provided.

Mr. Chairman, I am confident that we will ultimately prevail in our fight against terrorism, but we will do so only if we work together. Our agents must work closely with our local and state law enforcement partners -- our field offices must work with our Headquarters -- the Bureau must work with the CIA and our law enforcement and intelligence counterparts around the world -- and the counterterrorism components of the Executive Branch must have a meaningful and constructive relationship with our colleagues in Congress. These relationships are the lifeblood of our campaign against terror, and we must do everything in our power to sustain and nurture them.

TESTIMONY OF ROBERT MUELLER, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Director MUELLER. Thank you, Chairman Graham and Chairman Goss, Senator Shelby, Congresswoman Pelosi, and thank you for acknowledging the loss of our analyst, Linda Franklin, on Monday as a result of—at the hands of the sniper.

I want to thank you for the opportunity to appear before you this morning and to discuss the events of September 11, 2001, and most particularly to discuss the FBI's counterterrorism efforts since that tragic day.

I must start before addressing these matters, though, by taking a moment to honor the victims who died at the hands of al-Qa'ida terrorists on that day. We cannot begin to imagine how difficult this past year has been for those families. There can be no doubt that the pain, the anger, and the grief is as fresh today as it was on that Tuesday morning last year.

As we all know families lost mothers, fathers, daughters and sons and the public safety community lost courageous firefighters and law enforcement officers—all of them innocent people going about their daily lives. And we in the FBI extend our deepest sympathy to the surviving family members and the victims of those attacks and assure them that the FBI is determined to honor the memory of their loved ones by never wavering in our fight to address terrorism.

I would also spend a moment, if I could at the outset, recognizing the men and women of the FBI, particularly those serving as analysts and agents in the counterterrorism program. These are dedicated, hardworking, and most often underappreciated public servants who are devastated by the events of September 11.

These men and women have struggled day in and day out to do their jobs despite often inadequate resources and enormous workloads, and I over the past year have been honored to work alongside them, all of the men and women of the FBI. I do believe it is important to remind this committee and the American people that the mission of the FBI's counterterrorism program—to identify, prevent, deter and respond to acts of terrorism—is broad and multifaceted.

While the events of 9/11 have brought into focus the threat posed by Usama bin Ladin and the al-Qa'ida network, we must recognize, as George Tenet has pointed out, that the threats we face are not limited to one individual, one group or one country.

Our counterterrorism efforts must address the threats posed by a multitude of international and domestic terrorists. Our recent history reflects growing threats from a variety of such groups and individuals. Religious extremists including al-Qa'ida committed the bombings of the World Trade Center in 1993, Khobar Towers in Saudi Arabia in 1996, the embassies in Kenya and Tanzania in 1998, and the bombing of the USS *Cole* in Yemen in October of 2000.

More structured terrorist organizations were responsible for numerous other terrorist attacks. Hizbollah, for example, killed more Americans prior to September 11 than any other terrorist group, including al-Qa'ida—their 1993 truck bombings of the U.S. embassy and Marine Corps barracks in Lebanon, the 1984 bombing of

the U.S. embassy annex in Beirut, and the 1985 hijacking of TWA Flight 847.

And we cannot forget right-wing terrorist groups espousing principles of racial supremacy and anti-government rhetoric who have also in the past become a serious menace, as was so tragically evidenced by the April 1995 bombing of the Murrah Federal Building in Oklahoma City.

I should point out at the same time as George has that the FBI and our partners, the CIA and others, have prevented significant terrorist attacks—the 1993 plot to bomb New York landmarks, the 1995 plans to bomb United States commercial aircraft transiting the Far East, and the 1997 plot to place four pipe bombs on New York City subway cars, which was narrowly averted by the New York joint terrorism task force, the 1997 prevention of the possible detonation of 10 letter bombs at Leavenworth Federal prison and two offices of the Al-Hawat newspaper, and finally the 1999 investigation in coordination with the U.S. Customs Service, which resulted in the conviction of Akmed Ressam for a plot to bomb a Los Angeles International Airport at the turn of the Millennium.

I want to talk a moment about what the FBI has done subsequent to September 11. After the September 11 attacks, the FBI, the law enforcement community, and U.S. and foreign intelligence communities joined forces to find out everything that we could about the hijackers and how they succeeded. Our immediate goal was clear; that was to prevent another attack by fully understanding how the terrorists perpetrated this one. Thanks to these efforts and the unprecedented cooperation of the intelligence and law enforcement communities, both domestic and international, our investigation revealed many of the details about the planning, financing and perpetration of these attacks. Our investigation will undoubtedly continue and likely develop new and significant details in the years to come.

In earlier testimony before this committee and in my statement for the record I have explained much of what we now know about the hijackers' activities in this country—that they entered the country legally, that they committed no crimes with the exception of minor traffic violations, that they purchased airline tickets in cash or using the Internet and they dressed and acted like Americans merging into our society. And I do believe that the context in which these 19 individuals were able to come to the United States and take advantage of the liberties this country has to offer and operate without detection is important to a full understanding of how these attacks were successfully undertaken.

Now, in our post-September 11 investigative activity we have undertaken a number of investigations and operations that have dealt some blows to a number of terrorist groups within the United States. As all of us I believe are aware, two weeks ago the Joint Terrorism Task Forces in Portland, Oregon and Detroit, Michigan arrested four individuals who were charged with aiding and abetting al-Qa'ida fighters.

Last month the Buffalo, New York Joint Terrorism Task Force arrested individuals who were charged with traveling overseas in the summer of 2001 to attend the al-Farouq terrorist training camp located near Kandahar, Afghanistan. And in May Jose Padilla was

detained as he entered the United States from Pakistan at Chicago's—he was detained in Chicago's O'Hare International Airport. And last week in Chicago the Executive Director of the Benevolence International Foundation, a reportedly charitable organization, was charged in an indictment with fraudulently raising funds for al-Qa'ida and other violent groups. This was part of a—as charged, was part of a multinational criminal enterprise spanning over a 10-year period.

And I should also add and point out that over the last year, as a result of the U.S. military and Intelligence Community action in Afghanistan, Pakistan and other foreign lands, a large volume of paper documents, electronic media, videotapes, audio tapes and electronic equipment has been seized, and the FBI, CIA, DIA and NSA have established a coordinated effort to exploit these seized materials.

These are just a sampling of the investigative and preventive efforts that have borne fruit over the last year. There have been others, but those operations, many of them, remain classified and have been described in closed sessions with the members of this committee.

I want to talk for a moment and turn to the reforms made in the FBI in the wake of September 11. These 13 months since September 11 have been a time of great change for the Federal Bureau of Investigation. Starting immediately after the planes hit, over half of our 11,500 agents suddenly found themselves working terrorism matters. It became clear that our mission and our priorities had to change dramatically. Today the FBI has twice the number of agents permanently assigned to counterterrorism as were assigned prior to September 11, and other permanent changes have been carefully considered and implemented.

We have been addressing the shortcomings of the Bureau and the Intelligence Community that have been highlighted since the September 11 attacks, and we have heard and we acknowledge the valid criticisms, many of which have been reiterated by this committee. For example, the Phoenix memo should have been disseminated to all field offices and to our sister agencies, and it should have triggered a broader analytical approach, and the 26-page request from Minneapolis for a FISA warrant should have been reviewed by the attorneys handling the request in our FISA section. These incidents and others have informed us on needed changes, particularly the need to improve accountability, analytic capacity and resources, information-sharing and technology, to name but a few.

And we have taken steps to address these shortcomings, some of which I would like to briefly highlight today. First is the reorganization of the Counterterrorism Division. In November of last year, Congress approved my proposal for a reorganization of FBI Headquarters. Under this reorganization, the Assistant Director for Counterterrorism is responsible for management of the national terrorism program and for select cases and operations which require national level management due to special circumstances, situations or sensitivity.

This management structure is a recognition that counterterrorism has national and international dimensions that tran-

scend field office territorial borders and require centralized coordination to ensure that individual pieces of an investigation can be assembled into a coherent picture. This ensures accountability for the program. Under the prior system, whereby field offices would have primary responsibility for terrorism cases, responsibility was diffused and Bureau leadership could not easily be held accountable for the program. This organization, the Assistant Director for Counterterrorism is accountable for taking all steps necessary to maximize our counterterrorism capacity, and by saying that I don't mean at all to relieve myself of the accountability ultimately for that program, because I am the one ultimately responsible for its success or its failure.

One of the ways in which Headquarters supports the field now in maximizing the counterterrorism capabilities is through the newly created flying squads. These squads augment local field investigative capabilities with specialized personnel and they support FBI rapid deployment teams, thereby providing a surge capacity for quickly responding to fast-breaking situations in locations where there is no FBI presence.

Now, this committee is familiar with the FBI's analytical shortcomings, as demonstrated by the limited dissemination and analysis afforded the Phoenix memo. Over the last year, we have undertaken the following measures to enhance our analytical capability. First, we've created the Office of Intelligence, which is the component of the FBI that will oversee development of the analyst position and career track and will ensure that intelligence is shared as appropriate within the FBI and the rest of the United States Government. I'm grateful to Director Tenet for his willingness to detail experienced CIA managers from his Directorate of Intelligence to the FBI to set up and manage that office.

We have significantly increased the resources allocated to analysis. With regard to intelligence operations specialists, who provide direct support to investigations, we are proposing a total staffing level of 205, with 89 currently on board and 44 in various stages of background investigation.

With regard to the intelligence research specialists who provide strategic analysis, we are proposing a total staffing level of 155, with 70 currently on board and 73 in the background investigation process.

We have requested an additional 28 intelligence operations specialists and 114 IRS, intelligence research specialists, in our 2003 budget. And of course I'm concerned that until the 2003 budget is approved the FBI will be held to its current spending levels, which could have an impact on the development of our analytical program.

We have created a College of Analytical Studies to provide training for all FBI analytical support personnel. This college is intended to become a featured component of training at the FBI Academy, along with new agents training at the FBI National Academy. And through the efforts of our expanded Terrorist Financial Review Group and the interagency teams conducting document exploitation, we have augmented FBI capabilities to perform financial and communications analyses of terrorist groups and networks.

Much has been made of the reportedly hostile relationship and turf battles between the FBI and the CIA, and, as you've heard from Director Tenet, the relationship between the FBI and the CIA has never been stronger or more productive. We have to concede that there were in the past isolated failings in the information flow between the two agencies prior to September 11. We must not overlook the fact that a successful systemic effort has been under way for years to develop and build upon our agencies' relationship. Starting with Dale Watson's detail to the CIA's Counterterrorism Center in 1996, we have had a regular exchange of employees.

At this time, we have a number of FBI employees assigned to the CIA's Counterterrorism Center and the CIA has eight managers and dozens of analysts assigned to the FBI's Counterterrorism Division. Each of these employees has unfettered access to the computer databases and computer systems of the other agency, and every morning a CIA official detailed to the FBI joins other FBI executives in my office for briefings that occur twice a day.

This committee has also presented, I believe, select testimony that is critical of the FBI's historical unwillingness and technological inability to share information with not only the CIA but with other Federal agencies and with our State and local law enforcement colleagues. Since September 11, we have instituted several changes which have resulted in significant improvements in communication and coordination of many aspects of information-sharing. I'd like to summarize briefly some of those initiatives adopted since September 11.

We've established Joint Terrorism Task Forces in each of our 56 field offices. Prior to September 11, only 35 offices had those task forces, and this partnering of FBI personnel with investigators from various local, State and Federal agencies on these task forces encourages the timely sharing of intelligence that is absolutely critical to our counterterrorism mission.

We established a new Joint Terrorism Task Force at FBI Headquarters to complement task forces established in each of the FBI's 56 field offices and to improve collaboration and information sharing with other agencies. We currently have representation of 26 Federal agencies and two State and local law enforcement officials who on this task force report to the FBI's Command Center.

We have undertaken a Joint Terrorism Task Force information sharing initiative involving the St. Louis, San Diego, Seattle, Portland, Norfolk and Baltimore field offices. This pilot project, which was first initiated in the St. Louis office, will integrate extremely flexible search tools that will permit investigators and analysts to perform searches on the full text of investigative files, not just indices.

Fourth, we created the Office of Law Enforcement Coordination to enhance the ability of the FBI to forge cooperative and substantive relationships with all of our State and local law enforcement counterparts. This office is run by a former police chief. And we've established the FBI Intelligence Bulletin, which is disseminated weekly to over 17,000 law enforcement agencies and to 60 Federal agencies.

As a result of these initiatives and despite some of the testimony that this committee has heard, we have received numerous letters

of support and gratitude from State and local officials and most particularly from the International Association of Chiefs of Police. I would like to submit some of those letters to the committee and ask that they be included as part of the official record of this inquiry.

Chairman GRAHAM. Without objection, so ordered.

[The information referred to follows:]

Aug-26-02 09:09am From-

International Association of
Chiefs of Police

515 North Washington Street
Alexandria, VA 22314-2357
Phone: 703/836-6767; 1-800/THE IACP
Fax: 703/836-4543
Cable Address: IACPOLICE

President
William B. Berger
Chief of Police
North Miami Beach, FL

Immediate Past President
Bruce D. Glasscock
Executive Director
City of Plano
Plano, Texas

First Vice President
Joseph Samuels, Jr.
Chief of Police
Richmond, CA

Second Vice President
Joseph M. Polisar
Chief of Police
Garden Grove, CA

Joseph G. Estey
Chief of Police
Hartford Police Department
White River Junction, VT

Fourth Vice President
Mary Ann Viverette
Chief of Police
Gaithersburg, MD

Fifth Vice President
Lonnie J. Westphal
Colonel/Chief
Colorado State Patrol
Denver, CO

Sixth Vice President
Joseph C. Carter
Chief of Police
Oak Bluffs, MA

Emile Perez
Commissaire Divisionnaire
French National Police
Lognes, France

Vice President-Treasurer
Donald C. Pierce
Chief of Police
Boise, ID

Division of State Associations of
Chiefs of Police
General Chair
Russell B. Laine
Chief of Police
Algonquin, IL

Provincial Police
General Chair
James McMahon
Superintendent
New York State Police
Albany, NY

Parliamentarian
David G. Walchak
Deputy Assistant Director
Federal Bureau of Investigation
Washington, DC

Executive Director
Daniel N. Rosenblatt
Alexandria, VA

Deputy Executive Director/
Chief of Staff
Eugene R. Cromartie
Alexandria, VA

August 22, 2002

The Honorable Robert Mueller
Director
Federal Bureau of Investigation
Washington, DC

Dear Director Mueller:

On behalf of the International Association of Chiefs of Police, (IACP) I am writing to express our gratitude for all of your efforts to improve the FBI's cooperation, communication and coordination with state and local law enforcement agencies. I commend you for your leadership on this issue and applaud your determination to ensure that the FBI works hand in hand with state and local law enforcement.

Following the September 11th attacks, it became apparent that the crucial partnership between federal, state and local law enforcement was being hindered by difficulties in information sharing. Over the past few months, the IACP has shared with you our concerns on several important issues such as the manner in which critical information on suspected terrorists is disseminated, the integration and coordination of crucial law enforcement data networks like the Regional Information Sharing System and Law Enforcement Online, and the process by which state and local law enforcement executives can receive security clearances.

It is my belief that the steps you have taken have been very responsive to these concerns and clearly demonstrate the FBI's commitment to enhancing its relationship with state and local law enforcement and improving our ability to combat not only terrorism, but all crime.

In particular, the creation of the State and Local Law Enforcement Advisory Panel and the Office of Law Enforcement Coordination has demonstrated the increased commitment that the FBI has placed on working with its state and local counterparts. In addition, the appointment of Chief Louis Quijas to head the Office of Law Enforcement Coordination ensures that the FBI will understand and utilize the strengths and

capabilities of state and local law enforcement as it develops new strategies for combating crime and terrorism.

Once again, the IACP appreciates all of your efforts on this crucial issue. It is my hope that your efforts to improve coordination and communication between federal, state and local agencies will serve as a role model for the Department of Homeland Security and other Federal agencies to follow. We look forward to working with you closely in the future.

Sincerely,

Wm B. Berger

William B. Berger
President

MARYLAND CHIEFS OF POLICE ASSOCIATION

Since 1961

P.O. Box 4686
Largo, MD 20775
Phone: (301) 218-1745
Fax: (301) 218-1746

President
Kenneth W. Krause
Chief of Police
UMPD, College Park, MD

Vice President
James R. Cruse
Chief of Police
Greenbelt City, MD

Treasurer
G. Wayne Livesay
Chief of Police
Howard County, MD

Secretary
Fred Keeney
Chief of Police
Mt Rainier, MD

Sergeant-at-Arms
Douglas DeLeaver
Chief of Police
Mass Transit Administration, PD

Immediate Past President
Larry E. Harmel
Chief of Police
MD Transportation Auth. PD

Executive Administrative Officer
Morris A. Lewis
Retired Chief of Police

Counsel
Mark G. Spurrier, Esq.

December 20, 2001

Mr. Robert S. Mueller III
Director – Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue N.W.
Washington, D.C. 20535-0001

Dear Mr. Mueller:

On behalf of the Maryland Chiefs of Police Association, I wanted to congratulate you on your appointment as the Director of the Federal Bureau of Investigation. Our membership believes that your experience and leadership will provide the focus necessary to energize all law enforcement in the United States in the current war against domestic terrorism in our communities.

Your efforts in terrorism investigations in this country and abroad are recognized and applauded by local law enforcement and the hard work and dedication inherent in this battle has not escaped notice by the police chiefs represented by the Maryland Chiefs of Police Association. We are collaboratively sympathetic with the work load that recent events have placed on you and the staff under your command and offer our support of these efforts.

At our most recent Maryland Chiefs of Police quarterly meeting, the efforts of the Federal Bureau of Investigation were discussed, and the membership passed a unanimous resolution to support the Bureau in any way possible, as you coordinate the investigative efforts in the identification, apprehension, and prosecution of terrorist elements in the our respective jurisdictions. Our organization has requested that our member agencies respect the fact that some information regarding these terrorist cases and associated alert notices is confidential and not intended for dissemination outside competent authority within our agencies.

Mission Statement

"To unite law enforcement executives in delivering innovative, high-quality police services."

The Maryland Chiefs of Police Association will not join those factions critical of the Bureau response to internal terrorist activities and we collaboratively endorse the effort and strategy of the Federal Bureau of Investigation as it seeks to reduce the terrorist threat through the coordination of Bureau and local law enforcement assets. Our membership has been informed and recognizes, that as your agency collects and evaluates the vast amount of information pertaining to terrorism, the dissemination of this information will be made based upon your analysis of its applicability and suitability for dissemination at the local level.

I finally would like to offer an open invitation to meet with our membership when schedules permit. The Maryland Chiefs of Police Association represents the voice of the police chiefs in this state and our proximity to Washington, D.C. lends itself to personal interaction between you, your staff, and the local law enforcement officials supportive of the Bureau mission.

Sincerely,

Kenneth W. Krouse
President – MCPA

cc: Ms. Lynne Hunt

JAMES W. McMAHON
SUPERINTENDENT

NEW YORK STATE POLICE
BLDG. 22, 1220 WASHINGTON AVE.
ALBANY, NY 12226-2252

May 1, 2002

Honorable Robert S. Mueller III
Director
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue NW
Washington, D.C. 20535

Dear Director Mueller:

It was a pleasure seeing you at the Law Enforcement Advisory Group meeting you convened on April 24, 2002.

Obviously, all of us at the local, state and federal levels have much work to do in the counter terrorism area. To be successful, we have to move forward together, forgoing duplication and turf issues. I applaud you for your keen understanding of these points, and for the efforts you are undertaking to bring law enforcement together in the most efficient and effective manner possible.

As you are aware from our first meeting, we at the state and local level are interested in a smooth, two-way flow of information involving all 680,000 state and local law enforcement officers. To do this in an expeditious manner requires effectively linking information systems that involve wanted persons files (and other hot files), investigative databases such as the NCIC gang and terrorism file, and other investigative files such as those contained in RISS.

The key component is to interface these systems in an appropriate manner that establishes a critical information link to and from a patrol car using the existing NCIC and NLETS infrastructures. In this way (through either standard hit notifications, silent hits or investigative advisories), state and local NCIC inquiries that occur hundreds of thousands of times a day could be cross-checked against various databases, providing a powerful tool we have never before had at our disposal.

The presentation made by Mr. Ken Ritchart of your staff dealing with LEO, RISS and NLETS for horizontal information sharing can potentially incorporate these ideas and provide the basis for utilizing the 680,000 officers and their contacts in a manner that vastly improves the two-way flow of information and allows access to appropriate levels of information at the various tiers of our law enforcement infrastructure, from the officer roadside to a regional intelligence center to a high-level counter terrorism unit within the FBI.

The second area that would complete an almost seamless information sharing system, reducing duplication and confusion, involves your reorganization plan that was detailed by Pat D'Amuro at our meeting. I was very impressed by this innovative plan. An overarching federal level Joint Terrorism Task Force that involves other federal enforcement entities, the Attorney General's Office and the Office of Homeland Security, would improve the flow of two-way information by clarifying for state and local level officials where to go to share and receive information at the federal level.

I believe that the two initiatives presented by Ken Ritchart and Pat D'Amuro are complimentary components of an approach that, if implemented in a coordinated manner, will solve nearly all the information sharing problems we at the state and local level presented at the first meeting of the Law Enforcement Advisory Group. I would like to personally commend you and your staff for your willingness to not only listen to the needs of state and local law enforcement, but to also respond with the initiatives you are attempting to implement.

Sincerely,

James W. McMahon
Superintendent

Sheriff Kevin Beary
ORANGE COUNTY SHERIFF'S OFFICE

COMMANDER KEN GREGORY
Emergency Response Team

Sector One
1111 N. Rock Springs Rd.
Apopka, FL 32712

Office: 407-654-1008
Fax: 407-654-1005
Pager: 407-899-3387

06-14-2002

Director Robert Mueller
Federal Bureau of Investigation
601 4th, Street, NW
Washington, D.C. 20535-0002

Sir;

I am a commander with the Orange County Sheriff's Office, in Orlando, Florida. I began my law enforcement career in 1967 with the Orlando Police Department. I left that agency after 15 years to join the Orange County Sheriff's Office where I have served for the past twenty years.

During my 35 years as a law enforcement officer, I have worked with members of the Federal Bureau of Investigation many times. On each and every occasion I found the agents to be professional, competent and caring. Based on my experiences with agents from the FBI, I have a deep admiration and respect for the members of the Bureau.

Since September 11th, I have watched with disgust as members of the Media, Congress and other so called experts have ridiculed and maligned the Bureau. An accusation that the Bureau should have been able to predict what the terrorists planned to do with the information that was available at the time is absolutely ludicrous.

I believed in the FBI when I was a youngster growing up in then small town Orlando, I believed in the FBI when I was serving my country in Vietnam and I believe in the FBI as I now serve my community as a Law Enforcement Officer.

I know the men and women of the FBI are doing everything possible to track down and bring to justice any person that poses a threat to our country. I have great confidence in the men and women of the Federal Bureau of Investigation and honestly believe that our country's safety is in good hands.

Please pass on to the men and women of the FBI that their efforts are greatly appreciated and do not go unnoticed. As a Law Enforcement Officer and as a citizen, I believe that the Bureau is in the right place at the right time. Advise the agents to keep their chins up, we their brothers and sisters in the Law Enforcement community, have faith in their ability, judgement and commitment to the preservation of peace and the protection of life and property.

Respectfully;

Cmdr. Ken Gregory

Commander Ken Gregory
Emergency Response Team
Orange County Sheriff's Office
Orlando, Florida, 32801

INSTITUTE FOR INTERGOVERNMENTAL RESEARCH

Emory B. Williams
Chairman & Chief Executive Officer

D. Douglas Bodrero
President & Chief Operating Officer

Post Office Box 12729
Tallahassee, Florida 32317-2729
Phone (850) 385-0600
Fax (850) 422-3529
http://www.iir.com

June 24, 2002

Director Robert S. Mueller
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, DC 20535-0001

Dear Director Mueller:

Let me start by expressing my appreciation for the job you are doing as FBI Director. As fate would have it, you assumed your new responsibilities shortly before the tragic events of September 11, 2001, which forever changed America and subsequently changed America's premiere law enforcement agency as well. The bold initiatives you have taken, I believe, recognize the gravity of the future challenge for the FBI, and I am confident that your leadership will skillfully guide the Bureau through these turbulent times.

Since 1996, the Institute for Intergovernmental Research (IIR), in a cooperative effort with the FBI, has conducted anti-terrorism research and training. This program began with a domestic terrorism challenge after the Oklahoma City, Oklahoma, bombing. Then Assistant Director Robert Bryant of the National Security Division recognized the need for state and local law enforcement training in anti-terrorism investigation and prevention. Although resources were limited, Assistant Director Bryant graciously agreed to join IIR and the U.S. Department of Justice, Bureau of Justice Assistance (BJA), in offering State and Local Anti-Terrorism Training (SLATT) to law enforcement officers nationwide. Prior to the millennium, international terrorism targeting America was added to the SLATT curriculum, with heightened emphasis after the events of September 11. To date, the SLATT Program has trained over 22,000 state, local, and federal officers representing all 50 states.

BJA has continued funding for this critical program, and new courses are currently being developed to train narcotic officers to recognize terrorism indicators and establish relationships with the various Joint Terrorism Task Forces (JTTFs). Another program under development is the Train-the-Trainer initiative, which will provide the necessary tools for anti-terrorism training to state and local academy directors and agency in-service training units.

SLATT has been fortunate to have several highly competent and dedicated FBI agents assigned as liaisons to the program. We commend Unit Chief Jonathan Binnie, who has enthusiastically supported the SLATT Program. Both Executive Assistant Director Dale Watson and Executive Assistant Director Kathleen McChesney have also been very supportive and are deserving of commendation for their special efforts.

One of the main purposes of this letter is to recognize the efforts of Supervisory Special Agent David Crane, Unit Chief of the Counterterrorism Training Unit at Quantico, Virginia. SSA Crane was assigned as liaison to the SLATT Program shortly after September 11, just as SLATT was organizing six major anti-terrorism conferences in conjunction with the Regional Information Sharing Systems (RISS). Over 2,600 state and local officers attended these conferences that were held across the Untied States. SSA Crane was asked to make a presentation at each of the RISS conferences, explaining initiatives and changes within the FBI since September 11.

As you are aware, many in law enforcement were somewhat skeptical concerning the FBI's willingness to work more cooperatively with state and local law enforcement and to share information concerning the war on terrorism. SSA Crane prepared an excellent presentation explaining the changes within the Bureau, your new initiatives, the Bureau's reorganization, and your insistence on the FBI working more cooperatively in the anti-terrorism area. As your initiatives unfolded, SSA Crane continuously updated his presentation and even, on one occasion, purchased a zip drive using his own funds the night before his presentation in order to update the results of a news conference you held that day. I personally listened to SSA Crane's presentation at each of the conferences and can attest to the fact that he presented your initiatives in a positive and enthusiastic manner, ending each presentation with a testimonial concerning your support to accomplish the objectives detailed by your initiatives. While it is possible that some officers remain skeptical, program evaluations indicate a great appreciation for SSA Crane's candor and sincerity. The FBI can be justifiably proud of this dedicated, professional agent, as he represents the highest standards of the FBI.

SLATT is currently scheduling a series of anti-terrorism investigative workshops across the United States, again supported by BJA. I believe it would be beneficial to the training program and the Bureau for SSA Crane to continue his participation in this effort. The cooperative efforts of the FBI and IIR will make certain that this training program continues to have significant impact on the war on terrorism and better prepare state and local officers for their active participation. Should you or any members of your administration have any suggestions or ideas to further enhance the SLATT Program,

please feel free to communicate your desires to me. Once again, thank you for your tireless dedication and for the outstanding job you are doing of providing effective leadership to the FBI during these challenging times.

Sincerely,

D. Douglas Bodrero

DDB:gr
ltr db rm

cc: Executive Assistant Director Dale Watson
Executive Assistant Director Kathleen McChesney
Unit Chief Jonathan Binnie
Unit Chief David Crane

COPY
POLICE DEPARTMENT

July 25, 2002

Mr. Robert S. Mueller, III – Director
Federal Bureau of Investigation
FBI Headquarters
935 Pennsylvania Avenue, NW
Washington, DC 20535

Dear Director Mueller:

I recently had the opportunity to speak to Mr. Louis Quijas, Assistant Director for the Office of Law Enforcement Coordination, at the North Carolina Police Executives/Chiefs Summer Training Conference held in Atlantic Beach, NC. I have been acquainted with Louis since his appointment several years ago as the chief of police for the city of High Point, NC. He is an excellent choice for your executive staff and know his appointment will improve communications between the FBI and the law enforcement community.

Assistant Director Quijas suggested I write you about an experience I had in dealing with one of our local FBI agents within the past year. Although I do not recall the agent's name or if the contact was pre- or post-9/11, I do recall the facts of the contact. The local agent was coordinating with a fellow agent out of the Chicago Field Office in reference to a threat to a then unidentified Jewish Temple in our jurisdiction, Cary, NC. The agent had an address and asked me to assist in determining if there was such an entity at that location or any other in our area. I was able to find that there had, indeed, been a Jewish Temple sited temporarily at the address provided and that it had moved to a location in the county near our town. I called the agent back and relayed this information along with referring him to a colleague with the Wake County Sheriff's Office if further coordination with the primary agency with jurisdiction at the new location was needed.

What happened next is the reason for this letter. I expected no further explanation or conversation on the matter. Instead, the agent proceeded to advise me the reason for his inquiry which was related to an informant's tip that a group of suspected terrorists in the Chicago area had been overheard discussing an attack against a Jewish Temple in Cary, NC. The agent went on to explain that the information was not confirmed but he was checking out the information on this end of the case. The agent did not "remind" me of the need to keep the information confidential. He treated me with the courtesy and respect of a fellow law enforcement professional which I greatly appreciated.

TOWN of CARY
316 North Academy Street • Cary, NC 27513 • PO Box 8005 • Cary, NC 27512-8005
tel 919-469-4021 • fax 919-460-4904 • www.townofcary.org

I was surprised, but very pleased, the agent entrusted me with what was, obviously, sensitive information on this matter. Hopefully, with the many challenges facing our nation today, such open communications will continue. I feel such feedback can only strengthen the cooperation among law enforcement at all levels of government.

Our agency has always enjoyed a positive working relationship with our state's Charlotte Field Office, now under the leadership of SAC Chris Swecker, and our local Resident Agency, under the leadership of SSRA Frank Perry (Raleigh RA). If there is anything our agency can ever do on our end to further assist the Bureau, in any regard, please feel free to let us know.

With best personal and professional regards,

Winfield J. Hunter

Winfield J. Hunter (FBINA 165)
Chief of Police
(919) 469-4023
whunter@ci.cary.nc.us

wjh

OMAHA POLICE

City of Omaha
Mike Fahey, Mayor

Donald L. Carey
Chief of Police
(402) 444-5666
FAX: 444-4225

505 South 15th Street
Omaha, Nebraska 68102-2769
www.opd.ci.omaha.ne.us

Steve A. Coufal
Deputy Chief of Police

Barbara J. Hauptman
Deputy Chief of Police

Brenda J. Smith
Deputy Chief of Police

August 29, 2002

Mr. Louis F. Quijas
Assistant Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Dear Louis:

Thanks so much for taking time out of your busy schedule last Friday, August 23, to meet with me. It was a pleasure to see you again and recall pleasant experiences. I wish you the best of luck in your new position with the F.B.I.

Please be assured that you have many friends in the Omaha Police Department, if you need any assistance, or if I can help in any way in the future, please do not hesitate to call upon me.

Sincerely,

Donald L. Carey
Chief of Police

DLC:lbc
chf06007

A Nationally Accredited Law Enforcement Agency

CITY OF ORLANDO

OFFICE OF
GLENDA E. HOOD
MAYOR

August 5, 2002

Louis F. Quijas, Assistant Director,
Office of Law Enforcement Coordination
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001

Dear Director Quijas:

Thank you for your insightful remarks at our National League of Cities Board of Directors meeting in Minnesota. It is clear that, with your law enforcement background, you have a good grasp on the fullness of your responsibilities as the Assistant Director of the Federal Bureau of Investigation's newly created Office of Law Enforcement Coordination.

Knowing that the Office of Law Enforcement Coordination was created to enhance the coordination and communication between the FBI and state, municipal, county and tribal law enforcement on a national level, I am counting on you to serve as both a liaison and an advocate for state and local issues.

As we discussed in Minnesota, the safe and orderly flow of real-time intelligence information between federal and local government agencies is paramount to the safety of our homeland. An issue that continues to need the utmost attention is the void of security clearances being finalized for state and local officials who have been identified as needing clearances.

I am pleased to report that, in the City of Orlando, Officer Chris S. Berry of the Orlando Police Department who was appointed on October 4, 2001, as a Task Force Agent to the Orlando/Orange County Joint Terrorism Task Force of the FBI, just received his security clearance.

Since we both know the importance of security clearances, you can only imagine how Agent Berry and his counterparts on the task force are now better equipped to share information to fight the terrorist threat. I look forward to the other clearances following in a timely manner.

CITY HALL • 400 SOUTH ORANGE AVENUE • P.O. BOX 4990 • ORLANDO, FLORIDA 32802-4990
PHONE 407-246-2221 • FAX 407-246-2842 • http://www.cityoforlando.net

Additionally, the Memorandum of Understanding from the FBI for the task force was just received by the Orlando Police Department last month and the city legal staff is working rapidly to review and finalize the document for signatures.

My colleagues throughout the country and I look forward to working with you on the safety of our hometowns. Please don't hesitate to contact me for any assistance you might need now or in the future. In the meantime, I would like to extend an invitation to you to visit Orlando and meet with our local authorities and me to discuss ways for continuing to improve our methods of communication. Additionally, it would be beneficial to have you address the Domestic Security Advisory Panel, which I chair for our Governor, Jeb Bush. I will follow up with your office to get these plans in motion.

We need your guidance and support and we want our endeavors to be ones of success.

Most sincerely,

Glenda E. Hood

Glenda E. Hood
Mayor

Director MUELLER. We are also addressing the shortcomings of the Bureau's information technology. Over the years we have failed to develop a sufficient capacity to collect, store, search, retrieve, analyze and share information. Prior testimony before this committee has described the problems the FBI is experiencing because of outdated technology. Thanks to the support of Congress, the FBI has embarked on a comprehensive overhaul and revitalization of our information technology infrastructure. That process is well under way, but I want to caution you that these problems will not be fixed overnight.

Our technological problems are complex, and they will be remedied only through careful and methodical planning and implementation. We have made progress in the past year, and we have laid the groundwork for significant progress in the months and the years to come.

My prepared testimony sets forth additional details of the development and deployment of what we call the Trilogy Program, or revitalization of our technological infrastructure. It will create an automated system that will allow the FBI to share top secret and sensitive, compartmented information internally and throughout the Intelligence Community. In the wake of last year's terrorist attacks, the Congress has provided the additional funding we need to enable us to accelerate the implementation of some of these critical initiatives.

In conclusion, Mr. Chairman, we say that in the aftermath of September 11 the FBI quickly recognized that the organization needed to change in order to address the terrorist threat facing this Nation. As I've indicated, the FBI has faced many challenges over the past 13 months, and I believe we have made significant progress in addressing these challenges, but there is still a great deal of work to be done. I am, however, proud of the flexibility and the willingness of the FBI workforce to do whatever it takes to change whatever needs changing to prevent another terrorist attack.

I must say that despite our accomplishments and some of the successes we have had in reorganizing the FBI over the last year and in addressing our shortcomings, the transformation must continue. We must develop a workforce that possesses specialized skills and backgrounds, that is equipped with the proper investigative, technical and analytical tools and possesses the managerial and administrative competencies necessary to deal with a complex and volatile environment.

We are in the process of doing an internal reengineering to review and examine virtually every aspect of FBI operations, administration, policy and procedure. As a result of this review, we anticipate additional changes to FBI programs that will enable us to most effectively and efficiently utilize the tools and the resources Congress has provided.

And, Mr. Chairman, I am confident that we will ultimately prevail in our fight against terrorism, but we will do so only if we work together. Our agents must work closely with our local and State law enforcement partners, our field offices must work with our headquarters, and the Bureau must work with the CIA and our law enforcement and intelligence counterparts around the world.

The counterterrorism components of the executive branch must have a meaningful and constructive relationship with our colleagues in Congress. These relationships are the lifeblood of our campaign against terror, and we must do everything in our power to sustain and to nurture them.

And finally, once more let me say how immensely proud I am of the men and women of the FBI and all that they are able to accomplish under less than optimum conditions.

In closing, I would like to quote not a quote from me but a quote from one of the individuals who testified before you in the hearings, a New York field agent. When he testified before this committee, he presented his assessment of both the hearings and of his colleagues, and he said, "What has sometimes been lost in the media and in this inquiry process is that it's the same FBI, which has been extensively criticized since September 11, 2001, that is responsible for the investigation that led to the charges being brought against Zacarias Moussaoui." And he concludes, "The FBI is, of course, subject to human factors and limitation, and we are occasionally hamstrung by legal constraints, both real and imagined. But FBI personnel, both in the field and at FBI Headquarters were committed to preventing acts of terrorism prior to September 11, 2001, and we continue to be committed to that mission today."

Thank you, Mr. Chairman, and I'm prepared to answer any questions the committee may have.

Chairman GRAHAM. Thank you, Mr. Director. General Hayden.

[The prepared statement of General Hayden follows:]

STATEMENT FOR THE RECORD BY

LIEUTENANT GENERAL MICHAEL V. HAYDEN, USAF

DIRECTOR, NATIONAL SECURITY AGENCY/
CHIEF, CENTRAL SECURITY SERVICE

BEFORE THE

JOINT INQUIRY OF THE

SENATE SELECT COMMITTEE ON INTELLIGENCE

AND THE

HOUSE PERMANENT SELECT COMMITTEE

ON INTELLIGENCE

10 OCTOBER 2002

Introduction

1. Chairman Graham, Chairman Goss, and distinguished members of the Intelligence Committees, thank you for this opportunity to address you today. On behalf of the National Security Agency (NSA), I wish to extend our profound sympathy to the families of the victims and to the survivors of this terrible attack.

2. We know our responsibilities for American freedom and security at NSA. Our workforce takes the events of September 11, 2001 very personally. By the very nature of their work, our people deeply internalize their mission. This is personal.

3. Shortly after the attacks on the World Trade Center and the Pentagon, our director of Signals Intelligence (SIGINT) visited and calmed an emotionally shattered counterterrorism (CT) shop. That shop is located near the top floor of one of our high-rise buildings. For obvious reasons we had tried to move as many folks as possible into the adjacent lower buildings but we could not afford to move the CT shop. When I visited them later that afternoon, not only were they hard at work, they were defiantly tacking up blackout curtains to mask their location. Americans should be proud of these dedicated men and women who serve in the front lines of the war against terrorism.

4. This inquiry is very important, and it has played an important role for us and for the country in determining why al-Qa'ida was able to attack on that day with little warning and how we can better detect and defeat these kinds of operations in the future. Since April, we have hosted your staff in office spaces at our headquarters. We have shared data with them and—in response to their requests—have made available over 2,750 documents, some 15,000 pages of material, and arranged over 200 face-to-face meetings. We have assigned some of our best people to work full time with them. We have done this because—like you—we are committed to finding the full story of what led up to September 11th and to eliminating systemic problems that hamper our ability to aggressively collect against terrorists.

5. My goal today is to provide you and the American people with as much insight as possible into three questions: (a) What did NSA know prior to September 11th, (b) what have we learned in retrospect, and (c) what have we done in response? I will be as candid as prudence and the law

allow in this open session. If at times I seem indirect or incomplete, I hope that you and the public understand that I have discussed our operations fully and unreservedly in earlier closed sessions.

6. You well know the fragility of all that we do and how efforts measured in millions of dollars and thousands of man-years are turned to naught overnight when a story about communications intercepts appears in the press. Such leaks make the intelligence challenges that we face just that much more difficult and costly. A setback of inestimable consequences in the war against terrorism occurred when Usama bin Laden and his key lieutenants stopped using a phone following 1998 press reports of our intercepts.

7. You are also well aware that the nation's SIGINT effort has successfully thwarted numerous terrorist attacks in the past. While our successes are generally invisible to the American people, everyone knows when an adversary succeeds. NSA has had many successes, but these are even more difficult to discuss in open session.

What Did NSA Know Prior to September 11?

8. So, to the first question: What did NSA know prior to September 11th? Sadly, NSA had no SIGINT suggesting that al-Qa'ida was specifically targeting New York and Washington, D.C., or even that it was planning an attack on U.S. soil. Indeed, NSA had no knowledge before September 11th that any of the attackers were in the United States.

9. I have briefed the committees on one area where our performance—in retrospect—could have been better. Ms. Hill referred to this in her September 20, 2002 testimony: "Unbeknownst to the CIA, another arm of the intelligence community, the NSA, had information associating Nawaf al-Hazmi with the Bin Laden network. NSA did not immediately disseminate that information, although it was in NSA's database." This was not some culturally based "failure to share."

10. As you know, one of our "value added" activities is sorting through vast quantities of data and sharing that which is relevant, in a usable format, with appropriate consumers. In this case, we did not disseminate information we received in early 1999 that was unexceptional in its content except that it associated the name of Nawaf al-Hazmi with al- Qa'ida. This is not to say that we did not know of and report on him and other individuals. We did. In early 2000, at the time of the meeting in Kuala Lumpur, we had the al-Hazmi brothers, Nawaf and Salim, as well as Khalid al-Mihdhar, in

our sights. We knew of their association with al Qa'ida, and we shared this information with the community. I've looked at this closely. If we had handled all of the above perfectly, the only new fact that we could have contributed at the time of Kuala Lumpur was that Nawaf's surname (and perhaps that of Salim, who appeared to be Nawaf's brother) was al-Hazmi.

11. There is one other area in our pre-September 11th performance that has attracted a great deal of public attention. In the hours just prior to the attacks, NSA did obtain two pieces of information suggesting that individuals with terrorist connections believed something significant would happen on September 11th. This information did not specifically indicate an attack would take place on that day. It did not contain any details on the time, place, or nature of what might happen. It also contained no suggestion of airplanes being used as weapons. Because of the processing involved, we were unable to report the information until September 12th.

12. To put this into some perspective, throughout the summer of 2001 we had more than 30 warnings that <u>something</u> was imminent. We dutifully reported these, yet none of these subsequently correlated with terrorist attacks. The concept of "imminent" to our adversaries is relative; it can mean soon or simply sometime in the future.

13. These two reports have become somewhat celebrated so I would like to dwell on them for a moment longer. I will set aside the damage done to intelligence sources and methods when unauthorized information enters the public domain. I will also set aside the impact on the workforce I represent when something it has legitimately kept secret from our adversaries suddenly leaps into the media.

14. What is missing is a sense of how SIGINT is done. Thousands of times a day, our front-line employees have to answer tough questions like: Who are the communicants? Do they seem knowledgeable? Where in the conversation do key words or phrases come? What is the reaction to these words? What world and cultural events may have shaped these words? (You may recall that Ahmad Shah Masood, head of the Northern Alliance, was killed the day before.) How much of the conversation is dominated by these events and are any of the phrases tied to them?

15. And, if you were responsible for the management (or oversight) of NSA, you would have to ask other questions like: Where was the information collected? Were any of the communicants targeted? How

many calls a day are there from this location? In what languages? Hazzar? Urdu? Pashto? Uzbek? Dari? Arabic? Is there a machine that can sort these out by language for you, or do you have to use a human? If there is such a machine—does it work in a polyglot place where one conversation often comprises several languages? How long does it take NSA to process this kind of material? (After all, we are not the intended recipients of these communications). Does our current technology allow us to process it in a stream or do we have to do it in batches? When the data is processed, how do we review it—oldest to newest or newest first? And aside from how we normally process it, did the sequence change at 08:46 a.m. on September 11th? Without explaining the context in which SIGINT operates, unauthorized disclosures do not inform public discourse; they misshape it.

16. That summarizes what NSA knew about the hijackers prior to September 11th. We have diligently searched our repositories and we will continue to do so. We will, of course, provide your staff with any and all relevant information we uncover.

What Has NSA Learned in Retrospect?

17. Now let me now address the second question. What have we learned in retrospect? The primary lesson is that NSA was indeed on the right path—a path of transformation. Congressional leaders told me at our first meeting more than three years ago that the Agency had fallen behind and was in danger of irrelevance. The challenge was above all technological. As one Congressional leader put it, "You need to hit a home run your first time at bat."

18. The volume, variety and velocity of human communications make our mission more difficult each day. A SIGINT agency has to look like its target. We have to master whatever technology the target is using. If we don't, we literally don't hear him; or if we do, we cannot turn the "beeps and squeaks" into something intelligible. We had competed successfully against a resource-poor, oligarchic, technologically inferior, and overly bureaucratic nation state. Now we had to keep pace with a global telecommunications revolution, probably the most dramatic revolution in human communications since Gutenberg's invention of movable type.

19. To be sure, we were still producing actionable SIGINT—in some ways the best we had ever produced—but we were accessing and processing a smaller portion of that which could and should have been available to us. To put it succinctly, we did not know what we did not know.

Public commentary on this usually comes at us in the form of "the Agency has failed to keep up with technology." Actually, we have made substantial progress but I would agree that we have a long way to go.

20. We are digging out of a deep hole. NSA downsized about one-third of its manpower and about the same proportion of its budget in the decade of the 1990s. That is the same decade when packetized communications (the e-communications we have all become familiar with) surpassed traditional communications. That is the same decade when mobile cell phones increased from 16 million to 741 million—an increase of nearly 50 times. That is the same decade when Internet users went from about 4 million to 361 million—an increase of over 90 times. Half as many landlines were laid in the last six years of the 1990s as in the whole previous history of the world. In that same decade of the 1990s, international telephone traffic went from 38 billion minutes to over 100 billion. This year, the world's population will spend over 180 billion minutes on the phone in international calls alone.

21. It was clear to us that we had to recapitalize if we were to keep up. The danger was not that SIGINT would go away, but that it would cease to be an industrial strength source of American intelligence. It would, we feared, begin to resemble an intelligence boutique: limited product line, limited customer set, and very high unit prices.

22. By the end of the 1990s—with a budget that was fixed or falling and demands from our customers that were unrelenting—we attempted to churn about $200 million per year in our program. This meant taking money away from current, still active, still producing activities and investing those dollars in future capabilities. $200 million per year was far short of what we needed and, in fact, I could make only about one-third of that number stick as our program went through the Executive Branch and the Congress.

23. I went public with an aspect of this dilemma in an interview with CBS News that aired on "60 Minutes II" in February 2001. David Martin was pressing me about our technological challenge and he was using al-Qa'ida and Usama bin Laden as his examples. I pointed out that al-Qa'ida did not need to develop a telecommunication system. All it had to do was harvest the products of a three trillion dollar a year telecommunications industry—an industry that had made communications signals varied, global, instantaneous, complex, and encrypted. During that interview, David asked me for an assessment,

specifically about al-Qa'ida. I told him: "David, it's a dangerous world out there. I can't guarantee you—in fact, I would refuse to guarantee you—that even if we were at the top of our game, ill things won't happen to Americans. These are very dedicated, very dangerous adversaries. And we work very hard against them and they obviously work very hard to protect themselves against us."

24. Shortly after September 11th, I had a meeting of my senior leaders. I asked them the following question: Is there any part of our transformation roadmap that we should change as a result of the attacks? Unanimously, they responded, "No, but we need to accelerate these changes." With the money the President has requested and Congress has provided, we have done just that. We still have much to do but these committees know better than most the performance of NSA in the current war. I know in my heart that this level of sustained excellence would not have been possible without the business process, organizational, personnel, and operational changes we have set in place and you have supported.

What Has NSA Done in Response?

25. The final issue—what have we done in response—will allow me to give some specifics although I may be somewhat limited by the demands of classification. I will use some of the terms that Congress has used with us over the past year.

26. It was heartening, for example, to hear Congress echo the phrase of our SIGINT Director, Maureen Baginski, in the belief that we need to be "hunters rather than gatherers." She believed and implemented this strategy well before September 11th, and then she applied it with a vengeance to al-Qa'ida after the attacks.

27. Another part of our strategy for nearly three years has been a shift to a greater reliance on American industry. We have been moving along this path steadily and we have the metrics to show it. As you know, in project GROUNDBREAKER we have already outsourced a significant portion of our information technology so that we can concentrate on mission. We have partnered with academia for our systems engineering. I have met personally with prominent corporate executive officers. (One senior executive confided that the data management needs we outlined to him were larger than any he had previously seen). Three weeks ago we awarded a contract for nearly $300 million to a private firm to develop TRAILBLAZER, our effort to revolutionize how we produce SIGINT in a digital age. And last week

we cemented a deal with another corporate giant to jointly develop a system to mine data that helps us learn about our targets. In terms of "buy vs. make" (the term Congress has used), we spent about a third of our SIGINT development money this year making things ourselves. Next year the number will be 17%.

28. Congress has also said that we had listened in on "large volumes of phone calls from the part of the world where al-Qa'ida was located...but didn't focus on al-Qa'ida." That is, frankly, incorrect. Ms. Hill gives NSA good marks in her report for being aware of the Director of Central Intelligence's declaration of war on al-Qa'ida.

29. We were focusing on al Qa'ida. But did we have enough linguists and analysts focused on the problem? Clearly we could have used more, but if these hearings were about a war that had broken out in Korea or a crisis in the Taiwan Straits, if we had been surprised by conflict in South Asia, if we had lost an aircraft over Iraq, or if American forces had suffered casualties in Bosnia or Kosovo—in any of these cases, I would be here telling you that I had not put enough analysts or linguists against the problem. We needed more analysts and linguists across the Agency—period.

30. In that light, Congress has criticized us for a "failure to recruit," especially to recruit linguists and analysts. Let me try to present the facts on that. NSA recruiting for the decade of the 1990s was indeed minimal. The Agency accomplished the downsizing that was imposed on it in the easiest and most humane way possible—it shut the front door. But as these committees know, we turned the "recruiting corner" in 2000, and 2001 was actually a record year for Agency recruiting, the best in over a decade. On one day alone in February of 2001 we interviewed some 1,700 applicants. Before the attack in September 2001 we had brought more than 600 new people on board. By September 11th, we had reached a pause in our hiring. We had already reached the legally authorized personnel levels you had set.

31. With your help we have sustained our recruiting efforts in 2002. Well over 800 people have come on board this year and our goal for next year—if Congress gives us the additional billets we have requested—will be 1,500. NSA has received over 73,000 resumes since the 11 September attacks, and we have been very aggressively seeking the best and the brightest. We know we have a rare opportunity to shape the path of American cryptology for the 21st century.

Conclusion

32. I want to end by focusing on some comments made in recent hearings about NSA's "unwillingness" to share information. I need to be clear on this point. We are a SIGINT agency. Our mission in life is to provide information to all source analysts, military commanders, policy makers and others in the U.S. government. Our only measure of merit is the quality and quantity of information that we push out the door every day. As we speak, NSA has over 700 people—not producing SIGINT—but sitting in our customers' spaces explaining and sharing SIGINT.

33. There have been some special concerns raised about our willingness to share SIGINT with law enforcement. The fact is that NSA provides a significant amount of SIGINT to law enforcement every day. FBI headquarters routinely receives some 200 reports daily from us. When this is further distributed within FBI, the recipients may not realize it is SIGINT because it is handled in such a way as to protect sources and methods from being disclosed.

34. Much has been said in these hearings about a "wall" between intelligence and law enforcement. I will speak only of NSA but I think it fair to say that—historically—we have been able to be more agile in sharing information with some customers (like the Department of Defense) than we have with others (like the Department of Justice). This is not something that we created or chose. For very legitimate reasons, Congress and the courts have erected some barriers that make the sharing with law enforcement more careful, more regulated.

35. As a practical matter, we have chosen as a people to make it harder to conduct electronic searches for a law enforcement purpose than for a foreign intelligence purpose. This is so because law enforcement electronic searches implicate not only 4th Amendment privacy interests, but also 5th Amendment liberty interests. After all, the purpose of traditional law enforcement activity is to put criminals behind bars.

36. There is a certain irony here. This is one of the few times in the history of my Agency that the Director has testified in open session about operational matters. The first was in the mid 1970s when one of my predecessors sat here nearly mute while being grilled by members of Congress for intruding upon the privacy rights of the American people. Largely as a result of those hearings, NSA is governed today

by various executive orders and laws and these legal restrictions are drilled into NSA employees and enforced through oversight by all three branches of government.

37. The second open session was a little over two years ago and I was the Director at that time. During that session the House intelligence committee asked me a series of questions with a single unifying theme: How could I assure them that I was safeguarding the privacy rights of those protected by the U.S. constitution and U.S. law? During that session I even said—without exaggeration on my part or complaint on yours—that if Usama bin Laden crossed the bridge from Niagara Falls, Ontario to Niagara Falls, New York, U.S. law would give him certain protections that I would have to accommodate in the conduct of my mission. And now the third open session for the Director of NSA: I am here explaining what my Agency did or did not know with regard to 19 hijackers who were in this country legally.

38. When I spoke with our workforce shortly after the September 11th attacks, I told them that free people always had to decide where to draw the line between their liberty and their security, and I noted that the attacks would almost certainly push us as a nation more toward security. I then gave the NSA workforce a challenge: We were going to keep America free by making Americans feel safe again.

39. Let me close by telling you what I hope to get out of the national dialogue that these committees are fostering. I am not really helped by being reminded that I need more Arabic linguists or by someone second-guessing an obscure intercept sitting in our files that <u>may</u> make more sense today than it did two years ago. What I really need you to do is to talk to your constituents and find out where the American people want that line between security and liberty to be.

40. In the context of NSA's mission, where do we draw the line between the government's need for CT information about people in the United States and the privacy interests of people located in the United States? Practically speaking, this line-drawing affects the <u>focus</u> of NSA's activities (foreign versus domestic), the standard under which surveillances are conducted (probable cause versus reasonable suspicion, for example), the type of data NSA is permitted to collect and how, and the rules under which NSA retains and disseminates information about U.S. persons.

41. These are serious issues that the country addressed, and resolved to its satisfaction, once before in the mid-1970's. In light of the events of

September 11th, it is appropriate that we, as a country, readdress them. We need to get it right. We have to find the right balance between protecting our security and protecting our liberty. If we fail in this effort by drawing the line in the wrong place, that is, overly favoring liberty or security, then the terrorists win and liberty loses in either case.

42. Thank you. I look forward to the committees' questions.

TESTIMONY OF LIEUTENANT GENERAL MICHAEL V. HAYDEN, USAF, DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE

General HAYDEN. Thank you, sir. Chairman Graham, Chairman Goss, distinguished members of the Intelligence Committees, first of all, thank you for the opportunity to address you today, and first of all, on behalf of the men and women of the National Security Agency, I want to extend our profound sympathy to the family of the victims and to the survivors of these terrible attacks.

We know our responsibilities for American freedom and security at NSA. Our workforce takes the events of September 11 very personally. By the very nature of our work in SIGINT, our people deeply internalize their mission. This is truly personal for them.

Shortly after the attacks on the World Trade Center and the Pentagon, our Director for Signals Intelligence, Maureen Baginski, visited and combed an emotionally shattered counterterrorism office. That office is located near the top floor of one of our high-rise buildings. Now, for obvious reasons we had tried to move as many folks as possible into our adjacent lower buildings, but we really couldn't afford to move the counterterrorism shop.

When I visited them later that afternoon, not only were they hard at work, they were defiantly tacking up blackout curtains on their windows to mask their location. They remain equally hard at work today. Americans should be proud of these dedicated men and women who serve in the front lines of the war against terrorism.

This inquiry is very important to us. It has played an important role for NSA and for the country in determining why al-Qa'ida was able to attack on that day with little warning and how we can better detect and defeat these kinds of operations in the future.

Since April, we've hosted your staff in our office spaces at our headquarters. We've shared data with them and, in response to their requests, have made available nearly 3,000 documents, 15,000 pages of material, and we have arranged about 200 face-to-face meetings.

We've assigned some of our best people to work full time with your staff, and we've done this because, like you, we're committed to finding the full story of what led up to September 11 and to eliminating the systemic problems that hamper our ability to aggressively collect against terrorists.

Now, my goal today is to provide you and the American people with as much insight as possible into the three questions Ms. Hill raised earlier. First, what did NSA know prior to September 11? Second, what have we learned in retrospect? And third, what have we done in response?

Now I'll be as candid as prudence and the law allows me in this open session, but if at times I seem indirect or incomplete, I hope you and the public understand that I've discussed our operations fully and unreservedly in earlier closed sessions.

You well know the fragility of all that we do and how efforts measured in millions of dollars and thousands of manyears are turned to naught when a story about communications intercepts appears in the press. Such leaks make the intelligence challenges that we face just that much more difficult and costly.

A painful example of inestimable consequences in the war against terrorism occurred when Usama bin Ladin and his key lieutenants changed their communications practices following 1998 press reports of NSA intercepts. You're also well aware that the Nation's SIGINT effort has successfully thwarted numerous terrorist attacks in the past, and while our successes are generally invisible to the American people, everyone knows when an adversary succeeds. NSA has had many successes, but these are even more difficult to discuss in open session.

So, to the first question—what did NSA know prior to September 11—sadly, NSA had no SIGINT suggesting that al-Qa'ida was specifically targeting New York and Washington or even that it was specifically planning an attack on U.S. soil. Indeed, NSA had no signals intelligence knowledge before September 11 that any of the attackers were in the United States.

I've briefed the committees on one area where our performance in retrospect could have been better. Ms. Hill referred to this in her September 20 testimony when she said, "Unbeknownst to the CIA, another arm of the Intelligence Community, NSA, had information associating al-Hazmi with the bin Ladin network. NSA did not immediately disseminate that information, although it was in NSA's databases."

This failure to share, as it has been called, was not some culturally-based failure. As you know, one of our value-added activities is sorting through vast quantities of data and sharing that which is relevant in a usable format with appropriate consumers. In this case, we did not disseminate information we received in early 1999 that was unexceptional in its content, except that it associated the name of al-Hazmi with al-Qa'ida. This is not to say that we didn't know of him and report on him or other individuals. We did.

In early 2000, by the time of the meetings in Kuala Lumpur, we had the al-Hazmi brothers, Nawaf and Salim, as well as Khalid al-Mihdhar in our sights. We knew of their association with al-Qa'ida, and we shared this information with the Community. I've looked at this closely. If we would have handled all of the above perfectly, the new fact that we could have contributed at the time of Kuala Lumpur was that Nawaf's surname and perhaps that of Salim, who appeared to be Nawaf's brother, that their surname was al-Hazmi.

Now, there is one other area in our pre-September 11 performance that has attracted a great deal of public attention. In the hours just prior to the attacks, NSA did obtain two pieces of information suggesting that individuals with terrorist connections believed something significant would happen on September 11. Now, this information didn't specifically indicate an attack would take place on that day, and it didn't contain any details on the time, place or nature of what might happen. It also contained no suggestion of airplanes being used as weapons. Because of the nature of the processes involved, we were unable to report the information until September 12.

To put this into some perspective, throughout the summer of 2001 NSA had more than 30 warnings that something was imminent. We dutifully reported these, yet none of these subsequently correlated with actual terrorist attacks. The concept of "imminent"

to our adversaries is relative. It can mean soon or simply sometime in the future.

Now, these two reports have become somewhat celebrated, so I'd like to dwell on them just for a moment longer. I'll set aside the damage done to intelligence sources and methods when unauthorized information enters the public domain. I'll also set aside the impact on the morale of the workforce I represent when something they have legitimately kept secret from our adversaries for the better part of a year suddenly leaps into the public domain.

What I really want to talk about is something that is missing in our discussion, and that is the nature of SIGINT and how it is done. Thousands of times a day our front line employees have to answer tough questions like who are these communicants? Do they seem knowledgeable? Where in the conversation do these key words or phrases come? What is the reaction to these words? What world or cultural events may have shaped these words? You may recall that Sheik Massoud, the head of the Northern Alliance, was actually killed the day before. How much of the conversation is dominated by these events? And are any of the phrases contained in them tied to them?

And frankly, if you're responsible for the management or oversight of NSA, you would have to ask some other questions like where was the information collected? Were any of these communicants actually targeted? How many calls a day are there from such and such a location? In what languages—Hazzar, Urdu, Pashto, Uzbek, Dari, Arabic? Is there a machine that you can use to sort out these languages for you, or do you have to do that by hand?

And if there is such a machine, does it work in a polyglot place where one conversation often comprises several languages? How long does it take NSA to process this kind of material? After all, we all recognize we're not the intended recipients of these communications. Does our current technology allow us to process it in a stream, or do we have to do it in batches? When the data is processed, how do we review it? Oldest to newest or newest first? And aside from how we normally process it, did the sequence change at 8:46 in the morning of September 11? Without explaining the context in which SIGINT operates, unauthorized disclosures do not inform public discourse. They misshape it.

Now, that summarizes what NSA knew about the hijackers prior to September 11. We've diligently searched our repositories and will continue to do so, and of course we'll provide your staff with any relevant information we uncover.

Now let me address the second question. What have we learned in retrospect? The primary lesson is that NSA was indeed on the right path, a path of transformation. Congressional leaders told me at our first meetings more than three years ago that the agency had fallen behind and was in danger of irrelevance. The challenge above all was technological. Chairman Goss, as you told me in our first meeting, General, you need to hit a home run your first time at bat.

The volume, variety and velocity of human connections makes your mission more difficult each day. Look, a SIGINT agency has to look like its target. We have to master whatever technology the

target is using. If we don't, we literally don't hear him, or if we do, we can't turn his beeps and squeaks into something humanly intelligible.

Now, NSA had competed successfully for four decades against a resource-poor, oligarchic, technologically inferior and overly bureaucratic nation state. Now we had to keep pace with the global telecommunications revolution, probably the most dramatic revolution in human communications since Gutenberg's invention of movable type.

Now, to be sure, we are still producing actionable SIGINT, in some ways the best we'd ever produced, but we were accessing and processing a smaller portion of that which could and should have been available to us. To put it succinctly, we didn't know what we didn't know.

Now public commentary on this usually comes at us in the form of "The agency has failed to keep up with technology," or similar phrases. Actually, we've made some substantial progress, but I would agree we've got a long way to go. We are digging out of a very deep hole. NSA downsized about a third of its manpower and about the same proportion of its budget until the decade of the 1990s. That is the same decade when packetized communications—that is, that E stuff we've all been familiar with—surpassed traditional communications. That is the same decade when mobile cell phones increased from 16 million to 741 million, an increase of 50 times. That is the same decade when Internet users went from about 4- to 361 million, an increase of over 90 times. Half as many land lines, telephone land lines, were laid in the last six years of the 1990s as in the whole previous history of the world. In that same decade of the 1990s, international telephone traffic went from 38 billion minutes to over 100 billion. This year the world's population will spend over 180 billion minutes on the phone in international calls alone.

Now, it was clear to us we were going to have to recapitalize if we were going to keep up. Now the danger wasn't that SIGINT would go away. The danger was SIGINT would cease to be an industrial strength source of American intelligence. It would, we feared, if we didn't keep up, begin to resemble an intelligence boutique, limited product line, limited customer set and very high unit prices.

By the end of the 1990s, with a budget that was fixed or falling and demands from our customers that were unrelenting, we attempted to what we called churn about $200 million per year in our program. Now that meant taking money away from current, still active, still producing activities and investing those dollars in that recapitalization in future capabilities. $200 million a year was far short of what we needed, and in fact, I could make only about a third of that number stick as our program went through the executive branch and Congress.

I went public with an aspect of this dilemma in an interview with CBS News that aired on 60 Minutes II in February 2001. David Martin was pressing me about our technological challenges, and he was using al-Qa'ida and Usama bin Ladin as examples. I pointed out that al-Qa'ida did not need to develop anything, and it certainly didn't need to develop a telecommunications system. All

it had to do was harvest the products of a $3 trillion a year telecommunication industry, an industry that had made communications signals varied, global, instantaneous, complex and encrypted. During that interview David asked me for an assessment, specifically about al-Qa'ida, and I told him, "David, it's a dangerous world out there. I can't guarantee you—in fact, I would refuse to guarantee you—that even if we were at the top of our game ill things won't happen to Americans. These are very dedicated, very dangerous adversaries. And we work very hard against them, and they obviously work very hard to protect themselves against us."

Shortly after September 11, I had a meeting of my senior leaders. I asked them the following question: Is there any part of our transformation road map that we should now change as a result of the attacks? And unanimously they responded no, but we need to accelerate the changes.

With the money the President has requested and Congress has provided, we've done just that. We still have much to do, but these committees know better than most the performance of NSA in the current war, and I know in my heart that this level of sustained excellence would not have been possible without the business process, organizational personnel and operational changes we have set in place and you have supported.

Now the final issue, what have we done in response? I'll give some specifics, although I may be somewhat limited by the demands of classification, and for familiarity I would like to couch some of this in the terms that Congress has been using with us over the past year.

It was heartening, for example, to hear Congress echo the phrase of our SIGINT Director, Maureen Baginski, in the belief that we needed to be "hunters rather than gatherers." She believed and implemented that strategy well before September 11, and then she applied it with a vengeance to al-Qa'ida after the attacks.

Another part of our strategy for nearly three years has been a shift to a greater reliance on American industry for products and services they are better equipped to provide. We've been moving along that path steadily, and we have the metrics to show it. As you know, in Project GROUNDBREAKER we have already outsourced a significant portion of our information technology so that we can concentrate on mission. We've partnered with Johns Hopkins Applied Physics Laboratory for our systems engineering. I've met personally with prominent corporate executive officers. Larry Ellison of Oracle confided to me one evening that the data management needs we were outlining to him were bigger than anything he had ever seen.

Three weeks ago, we awarded a contract for nearly $300 million to SAIC to develop TRAILBLAZER, our effort to revolutionize how we produce SIGINT in a digital age, and last week we cemented a deal with IBM to jointly develop a system to mine data that helps us learn about our targets.

In terms of buy versus make, which is the terminology that Congress has used with us, we spent about a third of our SIGINT development money this year making things ourselves. Next year that number will be down to 17 percent.

Congress has also said that we had listened in on large volumes of phone calls from the part of the world where al-Qa'ida was located but didn't focus on al-Qa'ida. That is frankly incorrect. Ms. Hill actually gives NSA good marks in every port for being aware of the DCI's declaration of war on al-Qa'ida. We were focusing on al-Qa'ida.

Now, did we have enough linguists and analysts focused on the problem? Clearly we could have used more, but let me be frank. If these hearings were about the war that had broken out in Korea or the crisis in the Taiwan Straits that had taken us by surprise or if we had been surprised by a conflict in South Asia or if we had lost an aircraft over Iraq or if American forces had suffered casualties in Bosnia or Kosovo, in any of these cases I would be here telling you that I had not put enough analysts or linguists against the problem. We needed more analysts and linguists across the agency, period.

In that light, we've been criticized for our failure to recruit, especially to recruit linguists and analysts, and I will grant you that NSA recruiting for the decade of the 1990s was minimal to nonexistent. The agency accomplished the downsizing that was imposed on it in the easiest and most humane way possible. It shut the front door. But as these committees know, we actually turned the recruiting corner in 2000, and 2001 was actually a record year for agency recruiting, the best in over a decade. In one day alone, in February, February of 2001, we interviewed 1,700 applicants. Before the attack in September 2001, we had brought more than 600 new people on board.

Now, it is true on September 11, we had paused in our hiring. We had already reached the legally authorized personnel levels that you had set for us.

With your help, we have sustained our recruiting efforts in 2002. Well over 800 people have come on board this year, and our goal next year, if Congress authorizes the additional billets we have requested, will be 1500. In fact, we've already brought 85 more folks on board in the first 10 days of this fiscal year. NSA has received over 73,000 resumes since the September 11 attacks, and we have been very aggressively seeking the best and the brightest. We know we have a rare opportunity to shape the path of American cryptology for the 21st century.

I want to end by focusing on some comments in recent hearings on NSA's unwillingness to share information. I need to be clear on this. We're a SIGINT agency. Our SIGINT mission is to provide information to all-source analysts, military commanders, policymakers and others in the U.S. Government. Our only measure of merit is the quality and quantity of information that we push out the door every day. As we speak, NSA has over 700 people, 700 people not producing SIGINT but sitting in our customers' spaces explaining and sharing SIGINT with them.

There have been some special concerns raised about our willingness to share SIGINT with law enforcement, and the fact is that NSA provides a significant amount of SIGINT to law enforcement. FBI Headquarters routinely receives about 200 reports per day from us. Now, when this is further distributed within FBI, the re-

cipient may not recognize it is SIGINT because it is handled in such a way as to protect sources and methods.

Much has been said in these hearings about a wall, a wall between intelligence and law enforcement. Now I'll speak only of NSA. I think it fair to say that historically we have been able to be more agile in sharing information with some customers, like the Department of Defense, than we have with others, like the Department of Justice. This is not something we created. It is not something that we chose. For very legitimate reasons, Congress and the courts have erected some barriers that make the sharing with law enforcement more careful and more regulated.

As a practical matter, we have chosen as a people to make it harder to conduct electronic searches for law enforcement purposes than for foreign intelligence purposes. This is so because law enforcement electronic searches implicate not only Fourth Amendment privacy interests but also Fifth Amendment liberty interests. After all, the purpose of traditional law enforcement activities is to put criminals behind bars.

There is a certain irony here. This is one of the few times in the history of my agency that the Director has testified in open session about operational matters. The first was in the mid-1970s when one of my predecessors sat here nearly mute while being grilled by Members of Congress for intruding upon the privacy rights of American people. Largely as a result of those hearings, NSA is governed today by various executive orders and laws and these legal restrictions are drilled—drilled into NSA employees and enforced through oversight by all three branches of government.

The second open session for a Director about operational matters was a little over two years ago, and I was Director at that time. During that session, the House Intelligence Committee asked me a series of questions with a single unifying theme: how could I assure them that I was safeguarding the privacy rights of those protected by the U.S. Constitution and U.S. law? During that session, I even said without exaggeration on my part or complaint on yours that if Usama bin Ladin crossed the bridge from Niagara Falls, Ontario to Niagara Falls, New York, U.S. law would give him certain protections that I would have to accommodate in the conduct of my mission.

And now here I am for the third open session for the Director of NSA explaining what my agency did or did not know with regard to 19 Arabs who were in this country legally.

When I spoke with our workforce shortly after the September 11 attacks, I told them that free people always had to decide where to draw the line between their liberty and their security, and I noted that the attacks had almost certainly pushed us as a Nation more towards security. I then gave the NSA workforce a challenge. We were going to keep America free by making Americans feel safe again.

Let me close by telling you what I hope to get out of the national dialogue that these committees are fostering—and frankly I'm not really helped by being reminded that I need more Arab linguists or by someone second-guessing an obscure set in our files that may or may not make more sense than it did two years ago. What I really need you to do is talk to your constituents and find out

where the American people want that line between security and liberty to be.

In the context of NSA's mission, where do we draw the line between the government's need for counterterrorism information about people in the United States and the privacy interests of people located in the United States? Practically speaking, this line drawing affects the focus of NSA's activity, foreign or domestic, the standard in which surveillances are conducted, probable cause versus reasonable suspicion, for example, the type of data NSA is permitted to collect and how and the rules under which NSA retains and disseminates information about U.S. persons.

These are serious issues that the country addressed and resolved to its satisfaction once before in the mid-1970s. In light of the events of September 11, it is appropriate that we as a country readdress them and, as the Director of Central Intelligence said a few minutes back, we need to get it right. We have to find the right balance between protecting our security and protecting our liberty. If we fail in this effort by drawing the line in the wrong place—that is, overly favoring liberty or security—then the terrorists win and liberty loses in either case.

Thank you, and I look forward to the committee's questions.

Chairman GRAHAM. Thank you very much, General.

For hearings of the Joint Inquiry we have agreed that four members, two from each committee, will serve as lead questioners. Each will have 20 minutes. The designated lead questioners for today's hearings in order will be Senator Levin, Congressman Burr, Senator Thompson and Representative Harman.

Senator Levin.

Senator LEVIN. Thank you, Mr. Chairman, and first let me thank both our Chairmen and our Vice Chairmen for their steady and their determined leadership of this effort and also add my thanks to Eleanor Hill and her staff for their extraordinary effort.

Mr. Chairman, after months of investigation and numerous Joint Inquiry hearings, both open and closed, a fair reading of the facts has led to a deeply troubling conclusion. Prior to September 11, the U.S. intelligence officials possessed terrorist information that if properly handled could have disrupted, limited or possibly prevented the terrorist attacks. At crucial points in the 21 months leading up to September 11, this intelligence information was not shared or was not acted upon, and as a result numerous opportunities to thwart the terrorist plot were squandered.

I've put up here a blue chart and handed to each of you copies of those charts which track two of the hijackers, al-Mihdhar and al-Hazmi, who were the hijackers of American Airlines Flight 77, which attacked the Pentagon.

I understand from Mr. Mueller's prior testimony, September 25, that the travel of the 12 terrorists who constituted the "muscle" for the 9/11 hijackings may also have been coordinated by al-Mihdhar.

The charts contain in chronological order well-established and well-known facts. The backdrop is that we know that in 1998 the CIA had essentially declared war on bin Ladin and on al-Qa'ida. Then, in December 1999, there was a heightened state of terrorist alert due to the Millennium celebration. That was the environment in which the failures occurred.

An intelligence report was sent to the CIA and the FBI identifying four al-Qa'ida operatives who had links to the East African U.S. embassy bombings and stating that they were planning to meet in Malaysia. The Malaysia meeting was of significant importance, so much so that not only was the FBI notified, but the Director of the CIA was briefed about that meeting on numerous occasions.

The CIA monitored the meeting in Malaysia, which took place from July 5 to July 8, 2000, 20 months before September 11. And as a result of the monitoring, the CIA learned some important information. On January 5, the CIA knew the full name of one of the attendees at what they knew was an al-Qa'ida operatives meeting. His name was Mihdhar. The CIA also had his passport information, including a multiple entry visa for the U.S. Our staff has concluded that that information was not distributed to the FBI, but there is some dispute about that.

On January 9, the CIA learned the full name of Hazmi, another attendee at the al-Qa'ida operatives meeting, and learned that al-Hazmi had left Malaysia on January 8 with Mihdhar on the same flight, seated together.

Now, with this information and this state of concern, this high-level state of concern and a declaration of being at war with al-Qa'ida, the CIA did not put either al-Hazmi or Mihdhar on the watch list, and, again, according to our staff conclusion, the CIA did not tell the FBI all that the CIA knew, including that Mihdhar had a multiple entry visa to the U.S.

I want to first focus, Mr. Tenet, on the question of the watch list, which you have talked about in your testimony. What reason specifically here—I don't want just a general answer here, that there was a lot of workload and so forth, but what reason was given specifically by the CIA person responsible for putting that name on the watch list as to the failure to do so?

Director TENET. For not putting the name on the watch list? Our judgment is, in talking to everybody working at the time, that there were uneven standards, poor training and we didn't——

Senator LEVIN. For that specific failure? All those reasons for that specific failure?

Director TENET. Yes, sir. We did not—the people involved were people who have access—people we've talked to acknowledge that there were uneven practices, bad training and a lack of redundancy. The fact that they were swamped does not mitigate the fact that we didn't overcome that redundancy, a separate unit or better training for those people.

Senator LEVIN. Have you identified the person or persons who were responsible to put that name on the watch list? We know who is working this case?

My question is do you know the name or the names of the person or persons responsible for putting those names on the watch list?

Director TENET. Yes, sir. I think I have them.

Senator LEVIN. Then we come to March 5, same year, 2000, and the CIA learns some additional information, very critical information. On March 5, the CIA learns that Hazmi had actually entered the United States on January 15, seven days after leaving the al-Qa'ida meeting in Malaysia. So now the CIA knows Hazmi is in the

United States, but the CIA still doesn't put Hazmi or Mihdhar on the watch list, and still did not notify the FBI about a very critical fact, a known al-Qa'ida operative. We're at war with al-Qa'ida, a known al-Qa'ida operative got into the United States.

My question is, do you know specifically why the FBI was not notified of that critical fact at that time?

Director TENET. The cable that came in from the field at the time, sir, was labeled "information only," and I know that nobody read that cable.

Senator LEVIN. But my question is do you know why the FBI was not notified of the fact that an al-Qa'ida operative now was known in March of the year 2000 to have entered the United States? Why did the CIA not specifically notify the FBI?

Director TENET. Sir, we weren't aware of it when it came into headquarters. We couldn't have notified them. Nobody read that cable in the March time frame.

Senator LEVIN. So that the cable that said that al-Hazmi had entered the United States came to your headquarters, nobody read it?

Director TENET. Yes, sir. It was an information-only cable from the field and nobody read that information-only cable.

Senator LEVIN. Should it have been read?

Director TENET. Yes, of course, in hindsight.

Senator LEVIN. Should it have been read at the time?

Director TENET. Of course it should have been.

Senator LEVIN. My question is do you know who should have read it?

Director TENET. I don't know that, sir, but I can find out.

Senator LEVIN. Was somebody responsible to have read it?

Director TENET. Well, somebody should have read it, yes, sir. We need to also look at where it came into, but I can find that out for you.

Senator LEVIN. You don't know who that person was?

Director TENET. I do not.

Senator LEVIN. Should they have been watch-listed at the time, March of 2000?

Director TENET. Yes, sir, we have acknowledged that fact.

Senator LEVIN. Do we know who was responsible for watchlisting at that time, when Hazmi had entered the United States? This is another trigger point. They should have been watch-listed.

Director TENET. I don't know the answer to that question, but I will provide an answer.

Senator LEVIN. Next, on October 12, 2000, bin Ladin operatives attacked the USS *Cole*. The FBI, which investigated that attack, learned that a bin Ladin follower, Khallad, was the principal planner of the *Cole* bombing and the two other participants in the *Cole* conspiracy had delivered money to Khallad at the Malaysia meeting. Now, the FBI told the CIA about those facts. That information came from the FBI to the CIA. The CIA went back, reviewed the facts that they had about the Malaysia meeting again and, as a result of that review in January of 2001, the CIA determined that Khallad had actually been at the Malaysia meeting and that Mihdhar and Hazmi then, they knew, you knew, had been involved with the planner of the *Cole* bombing, actually been with the planner of the *Cole* bombing at the Malaysia meeting.

CIA again failed to put either Hazmi or Mihdhar on the watch list or to notify the FBI that Hazmi was in the United States. And my question is, do you know who was responsible for that failure?

Director TENET. Sir, can I take you back to the facts for a moment?

Senator LEVIN. Sure.

Director TENET. First of all, in terms of the identification of Khallad, actually, it was the FBI who provided the information to us, because we were in a joint meeting at the time—at a third country, because we were running a joint case with somebody who identified Khallad. And indeed in January of 2001, the legal attache from this third country writes messages to both our headquarters that after having been shown the surveillance photos of Kuala Lumpur, he made an identification of Khallad. So at that point, sir, both the CIA and the FBI know that Mihdhar was in Malaysia and that—in this time period, and that Khallad was in Malaysia this time period as well.

Senator LEVIN. Now, that is irrelevant to my point. What you did not notify the CIA of at that point——

Director TENET. No. The FBI.

Senator LEVIN. You did not notify, thank you, the FBI of at that point is that you knew that Hazmi was in the United States?

Director TENET. That's correct, sir.

Senator LEVIN. That is January now of 2001, another failure.

Director TENET. Sir, there are three instances, as I note in my testimony, three separate occasions.

Senator LEVIN. I know. My question, do you know who is responsible to notify the FBI at that time?

Director TENET. I don't, but I'll find out for you.

Senator LEVIN. Now we have a meeting in the year 2002 in New York City, and this is a meeting of a CIA analyst and FBI officials from the New York field office, which was the office investigating the *Cole* bombing, and the FBI Headquarters, including the FBI analyst on detail to the Counterterrorist Center at the CIA. The FBI agents on the *Cole* bombing pressed the CIA at that meeting for information regarding Mihdhar and the Malaysia meeting, but the CIA representative denied them that information. That is a very specific finding in the staff report, that there was a refusal to share that information relative to Mihdhar in Malaysia and as to why the CIA was tracking Mihdhar, at a June 2001 meeting on the specific request of an FBI agent in New York.

My question is, do you know why the CIA agent refused to tell the FBI agent what the CIA agent knew when the FBI agent specifically said why are you tracking Mihdhar?

Director TENET. We have—we're going to have a disagreement on the facts here. And here are the facts as I understand them. There were three people who left New York to go to Washington—Washington to go to New York that day. It was an FBI analyst from FBI Headquarters, an FBI analyst from our Counterterrorism Center and our analyst. They went up to discuss the *Cole* investigation.

The FBI analyst from FBI Headquarters brought the surveillance photos with her, and at the end of the conversation—and I've now talked to the people involved, Senator—the FBI analyst from FBI Headquarters handed the surveillance photos to the New York field

office personnel. There was some discussion about them. Indeed, they were talking about different people. Mihdhar was not who they were talking about in this meeting. When I asked our person at this meeting as to whether he was specifically asked about Mihdhar and Hazmi, he has no recollection of the subject ever being directed to him or ever coming up. So there's a factual issue here, and I've only talked to two of the people involved. I haven't talked to——

Senator LEVIN. Well, let me read you the staff report. The CIA analyst who attended the New York meeting acknowledged to the Joint Inquiry staff that he had seen the information regarding al-Mihdhar's U.S. visa and Hazmi's travel to the United States, but he stated that he would not share information outside of the CIA unless he had authority to do so. That is what he told our staff. Do you disagree with that?

Director TENET. Sir, I've talked to him as well.

Senator LEVIN. Do you disagree that he said that to our staff?

Director TENET. Well, no, I don't disagree he said it to your staff. I'm telling you what he told——

Senator LEVIN. Did he tell you something differently?

Director TENET. Yes, sir. He gave me a different perspective.

Senator LEVIN. So he told you and he told our staff something differently?

Director TENET. But I think it's important, sir——

Senator LEVIN. But our time is limited so let me just keep going. That is the answer, he told you something differently from what he told our staff.

Mr. Mueller, Director Mueller, at that June 11 meeting, did the FBI know that Mihdhar and Hazmi were at the January 2000 meeting of al-Qa'ida operatives in Malaysia?

Director MUELLER. I don't believe they did.

Senator LEVIN. So we still don't know in June of 2001 what the CIA has known for 15 months.

Director Mueller, after Mihdhar and Hazmi were placed on the watch list by the CIA on August 23, 2001, now they are on the watch list. It is August. It is less than a month before September 11. The FBI opened an investigation on Mihdhar, but not on Hazmi. Why did the FBI not try to locate Hazmi?

Director MUELLER. My understanding is that the information related to Mr. Hazmi was included in the file of Mihdhar and that efforts were made to locate both of them.

Senator LEVIN. Your understanding is there was an effort to locate Hazmi?

Director MUELLER. Let me just check. My understanding.

Senator LEVIN. Okay.

All right. I think that is something different from what is in our report, because the New York agent was asked to open an investigation on Mihdhar, not on both.

Director MUELLER. My understanding is that we made an effort to identify and locate both individuals regardless of whether or not the file may have been opened under one as opposed to the other.

Senator LEVIN. All right. Director Mueller, without alluding to names, I want to talk to you about the individuals that were mentioned in the Phoenix memorandum. There were 10 individuals

that were the subject of an Usama bin Ladin-related investigation. How many of those 10—none of those we know were hijackers, but some of them were standbys perhaps, sleepers perhaps, ready to participate perhaps.

Director MUELLER. We have no evidence of that, Senator.

Senator LEVIN. How many of them in your findings, in your investigation, how many of the 10 people listed in the Phoenix report were part of the bin Ladin conspiracy?

Director MUELLER. My recollection, we have subsequently identified one of those as being associated with al-Qa'ida. Let me just check one second.

It is a question that I am not—I did not necessarily anticipate. So I have not gone and checked whether or not the investigations in each of the other nine—one I have in my mind was associated—we subsequently came to find was associated with al-Qa'ida. As to the other nine, I don't believe we have found that they have—any one of them has been associated with al-Qa'ida. But I would have to check to make absolutely certain.

Senator LEVIN. This is a very critical fact. You have got a Phoenix memo, you have got 10 people listed by that FBI agent, you have a visit to the apartment house, you have bin Ladin pictures all over the apartment, you have the agent saying this should be shared with the CIA. That information wasn't shared with the CIA. You have 10 people named as going to flight schools, great deal of suspicion, and—okay?

Director MUELLER. I think that is reading into that memorandum more than is there.

We absolutely had an investigation going on an individual, a principal individual and other associates. But in terms of—I think you have to take each of those individuals and weigh the evidence against each of those individuals. All of them were attending flight schools.

Senator LEVIN. According to our information, as of May of 2002, four of those were under bin Ladin-related investigations. Do you have any different information from that?

Director MUELLER. I would have to go back and determine. It may well be that they are the subjects under bin Ladin. In other words, we could open a file and in the file identify the individual as possibly an associate or a subject that should be investigated for the possibility of being associated with bin Ladin. But that is far different than having evidence and information than the person is in fact a member of al-Qa'ida.

Senator LEVIN. How many are still under investigation for a bin Ladin-related matter?

Director MUELLER. Out of that Phoenix memorandum?

Senator LEVIN. Yes.

Director MUELLER. At least three.

Senator LEVIN. I think this is highly significant information, that you should be on top of this, okay?

Director MUELLER. We have a number of investigations going on around the country.

Senator LEVIN. I am talking about the Phoenix memo.

Let me ask both of you. I have asked you, Director Mueller, to release the Phoenix memo, to make it public, redact it and to re-

lease the Minneapolis e-mails, redacted; and they have not been released publicly. Why not?

Director MUELLER. Hold on one second. Senator, to the extent that there is no classification issue we have no objection to them being released. My understanding is they are going through declassification.

Senator LEVIN. All right. I have requested you to release them some time ago, and they should be released by now.

Director MUELLER. That doesn't mean that we are holding up the declassification process, Senator.

Senator LEVIN. Well, then who is?

Director MUELLER. I would have to check on that.

Senator LEVIN. Well, the committee has asked for this, too. This is not just my personal request. The committee has asked for the release of these documents, redacted, made available to the public. If we want to change the way that things operate around here, we are going to have to be open and we are going to have to hold some people accountable.

Last question. Director Tenet, how many people have been held accountable for failures?

Director TENET. I haven't held anybody accountable yet, sir.

Senator LEVIN. Director Mueller, how many people have been held accountable for failures?

Director MUELLER. Well, depends on your definition of accountable. But I would say that I have not held somebody accountable in the sense of either disciplining or firing somebody. I have made changes as a result of what this committee has found and as a result of what we found in our investigation of what we did well and what we did not do well in the days and the months prior to September 11.

Senator LEVIN. If changes are going to be real and are going to stick, in addition to all of the structural changes that you have talked about and all of the other things which you have described, we need openness. We need documents to be released, which should have been released by now, including the Phoenix memo and the Minneapolis e-mails. We have waited a year for those.

And I believe people who failed in their responsibilities have got to be held accountable. This is not a matter of scapegoating. This is a matter of accountability. There has been, I believe, too little effort made to pinpoint the responsibility. You don't even know the names of the people who are responsible for failures and no holding people accountable. We are not going to have real change unless we have that.

And I will close with that.

Director MUELLER. May I respond to that, Senator?

Senator LEVIN. I would be happy.

Director MUELLER. When it comes to accountability, if you take something like the Phoenix memorandum that came back into headquarters, there were two analysts in two separate units that looked at that. The procedures in place at that time did not require the unit chief or the section chief to review that memorandum.

Now, I am not going to take in an analyst who is doing what he or she is supposed to do under those procedures and hold that person, quote, accountable.

Senator LEVIN. I'm not suggesting you should, only the people who you find failed. I am not suggesting that if some didn't fail you hold them accountable. It is where someone, in your judgments, have failed. There should be some accountability. That is all that I am suggesting.

Director MUELLER. But, going back to accountability, it is important to recognize that we have to put in place procedures which assure accountability.

One of the things I mentioned in my opening statement was the requirement that the accountability be at headquarters, as opposed to not being diffused in the field. So we are addressing accountability appropriately so.

Senator LEVIN. I would ask unanimous consent, Mr. Chairman, that my list of the CIA failures and the FBI failures relative to these matters be placed in the record at this time.

Chairman GRAHAM. Is there objection?

Chairman GOSS. Mr. Chairman, I don't object to it, but I think it would be noted that they are as prepared by Senator Levin.

Chairman GRAHAM. That is correct.

Senator LEVIN. It is right on the chart that way.

Chairman GRAHAM. Without objection, so ordered.

[The information referred to follows:]

CIA and FBI Failures
1999
2000
2001

CIA and FBI Failures
2001

Chairman GRAHAM. Our next questioner will be Congressman Burr. But, before that, a couple of announcements. We now are past the originally scheduled break time. We have done a survey of our Members and there is a general consensus, although not unanimity, that we proceed without a lunch break.

I am going to suggest that, in deference to our panelists who have been with us now for more than two and a half hours, that we have a break of five minutes and then we will reconvene, with Congressman Burr to be the first questioner.

Once we complete the designated questioners and turn to the five minutes of questions by individual Members, let me list the first six who will question: Senator DeWine, Congressman Hoekstra, Congressman Peterson, Congressman Bereuter, Congressman Roemer and Senator Lugar. Those will be the six who will question immediately after the conclusion of the designated questioners.

We will take a five-minute recess.

[Recess.]

Chairman GRAHAM. I call the meeting to order. If we can locate the panel, our next designated questioner is Congressman Burr.

Mr. BURR. Thank you, Mr. Chairman, and my thanks to the ranking members. In addition, let me take this opportunity also to thank the joint inquiry staff under the direction of Eleanor Hill for a difficult process that they have gone through but one that has been very effective.

Mr. Chairman, I am convinced that these public hearings were created to explore what, if anything, went wrong in the days and the events that led up to September 11. I am convinced that additional review is likely and probably needed and that we will establish an independent commission to carry on the work of this joint inquiry and to review our agencies that were not the focus of this current inquiry.

What has gone unmentioned until today, and I would like to reinforce it, is how many times the system worked. Most members of this inquiry have spent time across this country and around the world with our Intelligence Community and law enforcement individuals inquiring about what they knew and when they knew it but, more importantly, what they needed.

What we heard was crucial, I think, to this inquiry. But what we saw was invaluable to the American people—members of our intelligence and law enforcement community working unthinkable hours in primitive surroundings without family and friends, things we all take for granted. I mention this to my colleagues because our focus shifted for the last 12 months to what happened. Their focus has been and continues to be on protecting the American people from the evil that exists globally.

Though mistakes were made that contributed to the 9/11 attack, the men and women who work on our, the American people's, behalf around the world do this with the resources and authorities that we supply; and let's not forget they are the best in the world.

As this committee, as this inquiry hands off the review to a commission, I hope we will, as Members, refocus on what we can do to compliment the dedication of so many around the world with the resources that fill the gaps that all of us know exist.

Having said that, Director Tenet, Director Mueller, let me ask you, one year later, in hindsight, what would you have done differently? Also, recognizing the fact, Director Mueller, that you weren't in your capacity, but if you will give us insight as to possibly where the Bureau should have changed earlier, if they should have.

I will turn to Director Tenet first.

Director TENET. I think that personally when I think about this the one thing that strikes me that we all just let pass from the scene after the Millennium threat was this fellow who tried to cross the border from Canada into the United States. There were no attacks. There were no Americans killed. We didn't have any hearings. We didn't talk about failures. We didn't talk about accountability. We just assumed the system would keep working because it prevented the last attack.

He tried to cross the border; and I think one of the things that everybody should have done is say what does this mean more carefully, rather than just moving from this threat to the next threat. Assuming that it had been disrupted, what does it mean for the homeland? Should we have taken more proactive measures sooner? Hindsight is perfect. But, it is the one event that sticks in my mind.

Second, and again hindsight is perfect, we should have taken down that sanctuary a lot sooner. The circumstances at the time may have not warranted, the regional situation may have been different, and after 9/11 all I can tell you is we let a sanctuary fester, we let him build capability.

And there may have been lots of good reasons why in hindsight it couldn't have been done earlier or sooner. I am not challenging it, because hindsight is always perfect, but we let him operate with impunity for a long time without putting the full force and muscle of the United States against him.

I just heard a discussion about, you know, which one of my people is accountable. I need to tell you something. We have gone through this exercise about how much people and how do you count them. The truth is, the people that have been working this are absolute heroes. If I reflect back on my own responsibility, I tripled the size of CTC, quadrupled the budget. In hindsight, I wish I had said, let's take the whole enterprise down and put 500 more people there sooner.

I couldn't make that choice at the time because of all of the other competing things that I had to do that everybody would hold me responsible against failing for. But, in hindsight, I wish we had thrown more people at it in some way to give those people the relief.

Because, you know, the tempo and the pace and the exhaustion, notwithstanding the fact that on the watchlist issue procedures may have not been perfect, it is not an excuse. They were exhausted. There were never enough of them. There were never enough of us, period, across the range of targets that we cover.

So I think about that as well.

The other thing that I would say to you, quite frankly, is there was never a systematic thought process to think about how you play defense. It comes back to the guy trying to cross the border.

You can disseminate all of the threat reportings you want. You can do the strategic analysis about airplanes. You can do the strategic analysis about car bombs, truck bombs, assassination attempts, fast boats and everything else. You can put all of that out there to people.

Unless somebody is thinking about the homeland from the perspective of buttoning it down to basically create a deterrence that may work, your assumption will be that the FBI and the CIA are going to be 100 percent flawless all of the time. And it will never happen. Notwithstanding all of the improvements we have made with your help, it is not going to happen.

I think one of the things that we have learned is, in hindsight, the country's mindset has to be changed fundamentally. No more sighs of relief. We are in this for a long time. We have to get about the business of protecting the country with the private sector, the chiefs of police, the State and locals now. Because the threat environment we find ourselves in today is as bad as it was last summer, the summer before 9/11. It is serious.

They have reconstituted. They are coming after us. They want to execute attacks. You see it in Bali. You see it in Kuwait. They plan in multiple theatres of operation. They intend to strike this homeland again, and we better get about the business of putting the right structure in place as fast as we can.

Mr. BURR. I will come back to you in a minute on the coordination and communication with local law enforcement.

Director Mueller.

Director MUELLER. Well, looking back at it and seeing what our greatest vulnerability was in retrospect, it was the fact that we had not hardened our cockpits. We had assumed that hijacker on a plane will want to get the plane to the ground. We, unlike the Israelis with El–Al, did not harden our cockpits. And all of the warnings that we got probably would not have led us, in that environment, to take the step of requiring airlines to harden the cockpits to prevent hijackers from coming in and taking over planes and crashing them into buildings.

That is—in retrospect, when you look back at it, you ask, what could have been done to prevent this attack? That is the one thing that as a country, as an industry, that could have been done to protect this type of occurrence.

Mr. BURR. Whose responsibility would that have been?

Director TENET. Can I say something to you, sir? Bob, excuse me. Unless the program is systematic, they watch all of this very carefully. It is not just about fixing one thing. You have to think about it from a systemic perspective. It is not just harden the cockpits. You have to look at the whole system. So if it is not being done simultaneously, the terrorist just sits back. If you look at how those people behaved, you understand how they have collected data against an open society for years. It is not just one thing or one system.

Director MUELLER. For the Bureau, from the perspective of the Bureau, that—the two I think critical changes necessary were, one, to adopt a new way of looking at managing cases. The Bureau traditionally has run cases through office of origin. Each individual Special Agent in Charge is in charge of the cases that arise in that

particular field office or that division, and there can be discussion and tension as to who gets the office of origin.

Well, New York did a terrific job as office of origin for UBL, but New York is one field office. When you are looking at international terrorism it is important for us as an institution to have centralized all information relating to UBL, whether it comes from Portland, Oregon, or Portland, Maine, or Miami or from Hamburg, Germany, or someplace else, centralized, not only centralized information flow but also centralized accountability for assuring that investigations, wherever they may pop up, have the required manpower to be addressed; and we as an institution have over the years placed the accountability in the field offices. Where on the national program we face a national security threat, the accountability in my mind should be at headquarters.

That is coupled with the necessity of having the information in a centralized database with a sufficient number of analysts and those analysts having the capability to generate the reports that an intelligence agency has traditionally done. We have not filled that void in the past.

We have to do a better job of gathering our intelligence, analyzing that intelligence, and disseminating that intelligence. Those are the two critical items I believe that the Bureau has to address in order to prevent—do the best that we can to prevent another circumstance such as that which happened on September 11.

Mr. BURR. Director Tenet, there are a number of things that we saw in the 1990s that would suggest that the likelihood of an attack was greater, and every several years that happened, but there is no doubt that you personally believed that we had reached a new level in December of 1998 when you made a statement that we were declaring war on al-Qa'ida. From the time that you made that declaration, what specific things changed within the CIA to reflect your concern over an imminent attack?

Director TENET. Well, first of all, you actually had a strategic plan that you put in place about how to attack the target, whose plan was to not only collect more intelligence but to get in the sanctuary and attack it and gain as much intelligence as you possibly can.

We have heard all of those stories about, well, they didn't speak the languages, they couldn't get in the target. So, number one, you have to have a plan. You have to hold yourself accountable to the plan. You have to personally lead the execution of the plan.

We put more people on it. We put as much money—we asked you for more money. We asked the administration for more money. We created a worldwide coalition of partners who we relentlessly badgered to say that you have to be in this fight with us to augment our numbers.

And the other thing is you have to—it is not just what goes on at headquarters in the center, it is what is going on in the field and trying to grow more case officers while you are fighting this, trying to grow more analysts as you surge overseas, trying to resurrect the clandestine human capability that, quite frankly, everybody had ignored. And we were in terrible shape.

So the whole focus is, build your infrastructure and get after this problem and bring as many people to the fight as you possibly can

around the world to augment your own numbers and keep your eye focused on the target and figure out what the right balance is between the people at headquarters and the field, to get the tools out there where the operations are run, where the tracing needs to be done and the technical operations.

All I can tell you is if you see the pace of operations that we are sustaining today, it is because the foundation was built, the plan was in place, and the dollars that have shown up have made an enormous difference in terms of flexibility. What we still don't have are enough people.

So we are going to rob—we are going to keep robbing people. We have 900 people in the Counterterrorism Center today. It is not enough. You have got hundreds more overseas working this target almost exclusively. What we need to keep calibrating is how much more can we do to do everything that we know how to do to stop the next attack.

Mr. BURR. Director Mueller, in the 1990s, we had the World Trade Center bombing. In 1993, we had the threat of airline use for attacks that came out of the trials in 1995. We had the threats on the New York tunnels in 1995. And I think both you and Director Tenet have alluded to others.

At an earlier hearing, Dale Watson, the head of CT at the FBI, said prior to 9/11 there was a 98 percent likelihood that the attack would be abroad.

Given the facts just covered and the targets being domestic, what process do you understand that the FBI went through to come to a conclusion that there was only a two percent likelihood that an attack would happen domestically here in the United States?

Director MUELLER. I am not actually certain as to how we—Dale came to the two percent.

I do believe, and I have heard, not being myself familiar with it or familiar with the warnings that were coming out during this summer leading up to September 11, and my understanding—and I think George can talk to it perhaps more than I—most of those or many of those warnings related to attacks overseas, and that may have skewed the analysis to believe that because we are getting those warnings in, they are talking about attacks overseas, there is a less likely—less of a likelihood that it will be in the United States.

Mr. BURR. Director Tenet said earlier one of the biggest mistakes was here we caught somebody crossing the border and we didn't ask enough questions or suspect what else might be there that was targeted here. We had already had example after example of domestic targets, whether the attacks were thwarted or not. I guess my question is, what more do we currently do within the FBI to analyze what the domestic threat is?

Director MUELLER. Well, there are a number of levels. I would reiterate, it is not just the FBI. Because part of one of the, I think, valid considerations or concerns over the years is that we have treated our intelligence and law enforcement on the one hand separate from our foreign intelligence. In other words, we have the CIA that looks overseas. We have the FBI that looks within the United States. And for a long time that worked, where you didn't have an issue such as counterterrorism which floods across borders.

So when we look at the threat against the United States now we take into account issues such as the bombing in Bali. That is significant with regard to the threat within the United States. We did not always do that, I don't believe.

Apart from that, we look at the vulnerabilities within the United States. We look at the various investigations, both preliminary and full, that we have around the United States to determine whether or not there is any threat information that comes out.

Where we have an issue that comes to the fore where we believe that there needs to be additional analytical research given to it, we now give it that analytical research. If you can recall back in the wake of September 11, there was some—I believe that there was the possibility of using crop dusters, and that had come out in a couple of threat warnings. And when that happens, we pull everything relating to crop dusters. We alert each of our field offices to go out and coordinate with each of the fields. When something like that comes along, we utilize both our people in the field as well as our analytical capability to put together a picture of what the actual threat is and integrate it with what George has from his people overseas.

Mr. BURR. Let me stop you there. I am running out of time, and there are a couple of areas I need to try to cover.

Director Mueller, we had the Chief of Police from Baltimore testify at one of the open hearings. And I think both you and Director Tenet, as well as I think most members on this inquiry, would say that we had a breakdown of communication and an inability to disseminate information and that contributed in some way, shape or form to September 11. This Chief of Police said, I thought after September 11 things would change and the communication between Federal and local would get better. The fact was, he came to testify to say that it hadn't. Is that a surprise to you, and what is being done to try to open up that line?

Director MUELLER. Well, I did indicate in my opening statement that there were selected witnesses called to testify. I don't believe that this particular witness is representative of the feeling in the field. Does his testimony surprise me? I would say probably not.

But I will tell you every time that I have—and I have reached out to this particular individual in the past and asked him to call me if there are any concerns. Whenever I have seen, either publicly or in testimony before this committee or another committee, that there is a police chief who is not getting what he or she wants, I have called, picked up the phone and called them to try to address those concerns.

Mr. BURR. But it is the intent of the FBI to open those lines of communication?

Director MUELLER. Well, let me finish by saying that I got—I don't know whether—I am not certain when this testimony was, probably in September. But it is a letter from William Berger, the President of the IACP. The letter praises us for the changes we have made to address this particular problem. I will just read one paragraph:

"It is my belief that the steps you have taken have been very responsive to these concerns and clearly demonstrate the FBI's commitment to enhancing its relationship with State and local law en-

forcement in improving our ability to combat not only terrorism but all crime."

I was at the IACP two weeks ago. I talked to the hierarchy, and I believe that they are supportive. There are isolated individuals throughout the United States who do not believe we are doing enough, and there are areas where we still have a ways to go, getting clearances for chiefs of police, exchange of information all the way down and getting it back up. We have a number of joint terrorism task forces that are working exceptionally well around the country. I think if you went to 9 or 10, or 99 out of 100, or 55 out of 56 you will find that State and local police are very supportive of the relationship.

There will always be one, there will always be two, and we try to address them as we come along.

Director TENET. Well, I think here is the place that I think that we can be very helpful to Bob and the FBI. I mean, look, let me just put it in a couple of ways. There is nothing ambiguous about the strategic threat or the targets that they are thinking about or what they are looking at. Who are the most important people in the battle? The most important people in the battle are the people on the street in localities around the country who actually know their street, actually know their neighborhood, actually know people coming in and out of those neighborhoods.

What we need to do is, if you build a system that basically is based on the old rules, then we are not going to meet their needs. We need to give them products that are content rich, that reveal nothing about sources and methods and methodologies, that allows them to understand what we are looking at so that they can be in tune to what they can do to help us.

It is critical for this to succeed. Some of the things we are doing together, there is a lot of strategic analysis, target-based analysis, all kinds of papers we have written, sharing with the FBI. We need to bring those people in, sit them down, educate them, and then provide training to their people about how to think about this target, and they've got a lot of other things to do. But the smartest guy is the cop on the beat, because he or she sees things that nobody in a Washington bureaucracy is ever going to see.

Mr. BURR. Thank you.

Mr. Chairman, you have been extremely generous with the time. I would only ask, as I end my questioning, I wanted to get into the communications between CIA and FBI and the FAA. We have tried for some weeks now to get from both agencies the specific communications that took place in the calendar year of 2001 from either of the agencies specifically to the FAA or to airlines; and if you two directors would help us at pushing that a little bit within your own organizations so that we can look at those documents and understand better what was shared with the FAA and airlines.

Director TENET. We will do that for the record, Mr. Chairman.

We do know—the other thing that you need to be aware of is there was in this time period, and continues to be, a very active counterterrorism group down at the NSC who convened all of the stakeholders, reviewed the bidding, and in part there were two advisories issued last summer. There was nothing specific, although there was a heightened period of alertness.

The result was two advisories. But we didn't have a specific to help them. And I think that we have FAA representatives in our center, and we will come back to you, because—but this is where homeland security is really going to make a difference.

Mr. BURR. Thank you. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Mr. Congressman.

Senator Thompson.

Senator THOMPSON. Thank you, Mr. Chairman; and, gentlemen, thank you very much and thank you for your public service.

Mr. Tenet, I would say to you that homeland security will make a difference if it ever passes.

I was stricken by the proposition earlier by one of the questions that we should have accountability. Frankly, I agree with that concept. But I must say that if the type of person in question was a part of the Homeland Security Department, under current law, you could look forward to one year's notice of their deficiencies, several levels of appeal, several hours or days before appeal examiners, and an average of about 18 months before you can do anything with that person.

Now this is the Department of Homeland Security that we are debating right now. And we have just been told by the Director of the CIA that we are about at the same level of concern as we were last summer, and we are debating issues like that, as to how many levels of appeal someone should have or whether or not the new office should have the flexibility to devise a new system that may have some semblance to this century. But we haven't gotten there yet. But perhaps your testimony today will help us get there.

I might ask you, Mr. Tenet, in view of your analysis of where we are in comparison to last year, I take note of what I believe I recall is the level of warning out of the Office of Homeland Security of yellow level, I believe, nationally. It doesn't seem that that is really consistent with what you said. Do you think the level should be higher or are we talking about different things?

Director TENET. Sir, Tom Ridge and I will be meeting this afternoon. He has already taken measures in specific sectors where we are most worried about. There will be another discussion this evening and tomorrow.

But I would note to you, when you see the multiple attacks that you have seen occur around the world from Bali to Kuwait, the number of failed attacks that have been attempted, the various messages that have been issued by senior al-Qa'ida leaders, you must make the assumption that al-Qa'ida is in an execution phase and intends to strike us both here and overseas. That is unambiguous as far as I am concerned.

The government has taken measures already in specific areas where the intelligence was most credible and in sectors that we are most worried about. So we will continue to talk about this. But I am deeply concerned about where we are and the time period ahead of us.

Senator THOMPSON. So you are looking at concerns both within the United States, Continental United States and abroad?

Director TENET. Sir, one of the things that we can never forget is the specificity of what we see overseas may not be matched by the specificity of what you see here. If you go back to the narrative

before 9/11 and you saw what was going on overseas, you must make the analytical judgment that the possibility exists that people are planning to attack you inside the United States, multiple simultaneous attacks. We are the enemy. We are the people they want to hurt inside this country. So we extrapolate, but in the world I live with you have to pay attention to what is going on overseas.

Senator THOMPSON. Well, I don't think you could be any clearer, Mr. Tenet; and I think you were pretty clear in the summer of last year. I don't know in my recollection how public you were about that, but my recollection is that within the Intelligence Community and with regard to the administration and others, you made that assessment at that time, too; is that correct?

Director TENET. Yes, sir.

Senator THOMPSON. Let me ask you along those lines something that I think that we are all wondering, and that is what we have a right as a nation to expect out of our Intelligence Community. It seems to me that, on occasion, the Community has gotten very, very good intelligence.

My recollection is that before the attack on the USS *Cole* that we had a lot of information that we were in danger in that area. We knew that Yemen was a hotbed. We knew that our presence was targeted. And all of that before September 11 of last year.

We also had lots of information and, in fact, we had lots of patterns—patterns, dots within a sea of patterns and dots. But there were some emerging patterns, such as New York, such as Washington, DC, such as our infrastructure, such as airplanes, things of that nature; and it built pretty much to a crescendo right at that time.

So it seems to me like that on more than one occasion we have gotten a lot of information, a lot of it is in the ball park, a lot of it turns out to be good information, and that we have even been able to separate it out from all of the vast volumes of information that come in. But we can't pinpoint times and places.

We all know how difficult that is. We all know that this information is coming in along with lots and lots and lots of other information. One of you gentlemen has said in times past that you were actually drowning in information.

We also had a lot of general information, I might add, about the nature of the attack, the fact that Usama bin Ladin had held a press conference in 1998 saying he was going to attack us. You declared war in 1998. In effect, all of that is out there.

Yet, the question is, how much good does that do us unless we can take that next step? Are we entitled to expect that next step? What do we have a right to expect of our Intelligence Community with regards to predicting time and place of a major terrorist attack?

Mr. Tenet, I will ask you first.

Director TENET. It is the most difficult thing to do, is to have that date, time and place of event. You have to be able to take all of this data. You have to be able to then analytically assess a target set that it may be applied against. You have to go protect that target set. Because the truth is, is there will be dates and times and all kinds of information. It will never happen on the date and

time. And then the date and time will elapse; and then people will say, it is not going to happen. You have to expect us to tell you honestly in strategic terms, this is where the sector of the attack is going to be. That is what I know their training and methodology has been. This is my best judgment about what you have to go protect. Go protect it.

Now, in the overseas environment today it would be useful at some point to come out and sit down. There is a great deal of specificity overseas about places and times and events, and the pattern of racing to stop it has been pretty successful. You go back and look at this recent French tanker, and the reporting out there on the French tanker was two or three months old, but it was there. This is a place and a location that we are worried about, commercial shipping and tanker traffic, and so you see it stretches out over time.

What we owe you always and what we have to work harder to do is our best strategic judgment about what the "it" is.

Senator THOMPSON. Are we getting any closer? You talked about isolating sectors. Because before September 11, with all of that information out there that you had collected, you still weren't at all sure that it was going to be domestic. In fact, I think it is fair to say most people thought it would be foreign. And right up until very close to the end, we were talking about against the United States or Israeli interests. We weren't even sure that it was United States. So we getting any closer to pinpointing the sector, the country, domestic or foreign, city, anything of that nature?

Director MUELLER. Sir, you are getting—by virtue of what you have done in Afghanistan, by virtue of the over 3,000 people we have taken into custody around the world, by virtue of the senior leadership that we are all getting information from today, the texture and quality when coupled to the real-time intelligence collection is an order of magnitude different than it was before 9/11. The quality and your knowledge is miles down the road and the pace of operations around the world has given us an enormous amount of information that really allows us to think about this in a much more strategic and focused way. And we are getting better.

But to come back to your homeland security point, you better get that done. Because the strategic threat is unambiguous. You better have the mechanism in place to start locking down where we can tell you. And we think with some high confidence we can work with the private sector and go through sectors and identify vulnerabilities to say, go lock it down now. Don't wait for us to come tell you it is on top of you, because you can't work that way, sir.

Senator THOMPSON. I might point out, too, that some of the things we are trying to do in homeland security will not be within any continuing resolution. And passing of continuing resolutions, even if we do something later, is just going to move the solution further down the road.

Under the category of things we have learned, I would like to try something out on you and get your various reactions, anyone who wants to react.

It seems that our Nation is dangerously slow to react to a major threat to our national security. You mentioned the sanctuaries. As

I look at this in terms of accountability, I look at a lot of different places. I look at the executive branch. I look at the legislative branch. I look at the organizations that you gentlemen represent.

But with regard to the executive branch, we watched—correct me if I'm wrong—we watched Usama bin Ladin build an army and indoctrinate, train and build an army basically for five or six years in Afghanistan; did we not?

Director MUELLER. Yes, sir.

Senator THOMPSON. If we had a perfect Intelligence Community here, could we protect ourselves if we allowed sanctuaries such as that?

Director MUELLER. No.

Senator THOMPSON. Well, moving down a little bit further, we know that it is not just Afghanistan; we know that there are friendly countries, friends of ours, that to one extent or another are allowing terrorist presence. They allow free passage. The Bremer Commission has pointed this out.

We depend on them, as you have pointed out, and have depended on them for so much of our successes in cooperation. But I wonder if, regardless of what kind of cooperation we might get on individual cases, these so-called friendly countries or allies, can we fully address the problem until we convince those countries, many of them with growing Muslim populations—I am not sure that that is going to reverse itself—some of them under political pressures until they start cooperating more with us?

I notice in 1996 Congress authorized the President to delineate these countries as not cooperating fully. I don't know that that has been utilized at all. Can we give our friendly countries a pass on this? Are we inviting another level of sanctuary? It might not be a country taken over, but it doesn't have to be in order to pose a big danger. Where do we stand on this?

Director MUELLER. Sir, I would say that, number one, you—we do not have the luxury of basically walking away from any of these places and not continuing to press them to do better all of the time. There is no alternative. So engagement is absolutely the key here.

In the pre-9/11 environment there were lots of people around the world who believed that this was all about killing Americans or killing Israelis; it is not my problem.

Everybody's mindset has now been transformed. You have got to do this with the carrot; and if there is a stick, you have to have a stick. We have to stay engaged in places where you can—we can't be a hundred thousand people all around the world. You need to get into those places and have those societies change their laws.

There are a series of policy questions here, sir, as well in terms of how the transformation of these societies occurs so that they don't remain as feeding grounds of terrorists. But you have got to engage.

Senator THOMPSON. Well, let's move to Congress. It seems to me that we have had national intelligence estimates at least since the mid-1990s telling us about our vulnerabilities, like Washington, D.C., New York. We have had various commissions talk about this. We have been very slow to react. I remember Senator Lugar back during the Presidential campaign in the mid-1990s was talking about these things. Nobody paid any attention to these things. Na-

tional security issues were like three percent in the public opinion polls; and we responded—both branches of government responded accordingly.

You mentioned our history in terms of appropriations. I wish you could clarify, perhaps all of you gentlemen, this issue a bit for me. I look at these charts that you have there. I see chart 3, I believe, counterterrorism money appropriated to the Intelligence Community. And I know we can't talking about real numbers here. You got the big supplemental in 1999.

Director MUELLER. Sir, I don't have your charts. But——

Senator THOMPSON. Let me generalize. I think you will agree with me. It looks like, for the Intelligence Community generally speaking, there has been an upward trend in terms of counterterrorism money. I think you acknowledged that earlier.

The CIA—I look from the last decade—your appropriation has been at least as much as your request in about every year. 1995 was an exception. A lot of years your appropriation was more than the request, if you include supplementals in the later year.

Is it a fact that intelligence appropriations, in general, have been going down while counterterrorism funding has been going up? And, if so, what are we to make of that? Does that mean that we should not have been hamstrung in any way in terms of our counterterrorism efforts, or are you robbing Peter to pay Paul? Does that mean that while we are all focused on counterterrorism issues that there are some extremely important things out there not being done that may turn around and bite us in future years? What are we to take from these numbers?

Director TENET. Well, it means all of those things.

The other thing that I would take from those numbers is when you look back and reflect on where this all started, we had to do three or four things simultaneously. One, you had to pursue this target and the other targets that you say are important and indeed are important. You had to fix your infrastructure. You had to grow your workforce. But you had to resuscitate—in our case, you had to resuscitate your HUMINT capability, because the peace dividend in the 1990s said we are not doing this anymore.

Now in 1997 we had a strategic plan to resuscitate all aspects of this; and, you know, there is a cost associated to it. Now there were budget caps.

Senator THOMPSON. You had to rebuild your clandestine services. You had satellite difficulties.

Director TENET. The only point that I would make about the supplementals is, the only reason we got where we needed is Congress gave us those supplementals. It is an appropriate——

Senator THOMPSON. But intelligence cannot live on supplementals.

Director TENET. It is either programmatic, it is deep and it is long, or basically what happens when you get a supplemental, then the question is the next year when the budget submission doesn't reflect the supplemental or its operational tempo, we are starting all over again from the same place. You knew it, and we knew it.

Senator THOMPSON. It is not conducive to long-range planning?

Director TENET. No, sir.

Senator THOMPSON. Moving to your own agencies, we have talked about the deficiencies. I think one of the greatest concerns that we have in looking forward, in trying to decide where we need to make our improvements, still has to do with the gaps. You know, it is interesting that there are some memos, some public, some not public, that indicate that each of your agencies have had outstanding people doing outstanding work. We are right on the money. We are pulling things together the way that they should and drawing conclusions that they should have drawn.

But some cases weren't disseminated properly. In some cases it wasn't handed off to the right people. We know the story. But it is not like there are individuals out there that are incapable of doing this. It seems to be a systematic problem.

I am wondering where we stand with regard to that. My concern is this basically a coordination issue. We have seen instances, and we know of other instances that we have not had public, where there have been gaps. We have got a system—we all know that we have a system of, foreign is over here and domestic is over here. We are supposed to hand things off. We also know that we have a system whereby the lead agency here, the FBI, that is going to be charged with looking at this threat domestically and doing something about it has always been a law enforcement agency.

My concern is that we are asking the FBI to change its nature on a dime, as it were, from an after-the-fact investigative body that has been legendary for years and years in this country to a before-the-fact prevention body. And we think, perhaps, that by making some organizational changes at the top and by having some joint task force and things like that that will change the culture.

But the FBI has certain limitations because it is a law enforcement body. For example, when you are looking at somebody, you look at them. If you don't have hard evidence, you can look at them in terms of a preliminary inquiry for how many days? So many days. Then you have to either open up a full field investigation on them or drop it altogether.

I am wondering what motivation in an organization that is like this, what motivation in an organization that rewards cases being made, and people are known and rewarded and recognized for the cases that they have made and that they work on, what motivation is it for people around the country to be handing up tidbits of information that doesn't necessarily make sense to them, they don't know if someone else needs it. But our investigators are still talking to agents out in the field who don't feel any real sense or reprioritization out in the field.

It is a culture. I am convinced that it is not a matter of turf as such. It is not a matter that people deliberately try to keep things from people. But you have practices such as sources and methods principles, need-to-know principles, things of that nature.

You are trying to change an awful, awful lot, Mr. Mueller, it looks to me like, to cure, you know, your own problems. Then you are going to have to take the extra step, all of you, together to fill in these gaps, when each of you have your own analysts, each of have your own piece. We don't know whether or not it is going to work. I can't say it won't. You can't say that it will. But it looks to me like that there is something to be said for perhaps another

entity that is analysis oriented, that does not have law enforcement responsibilities or even collection responsibility but is analysis oriented that has the authority to task gaps as they find them.

I don't think we have anything like that now. I don't know whether that is comparable to MI–5 or any other models. I know it is difficult as we go along to maybe recognize that the structure that we know perhaps is not the one that needs to take us into this century. And I know I am laying an awful lot on the table here with one question.

But I will stop now and ask your thoughts on all of that. Do you really feel like the things you are doing now are going to cause this long history and these monumental difficulties to change, and can't we do better with a different pattern?

Director MUELLER. Well, let me start by addressing the issue of the culture. A lot of people talk about FBI culture, not sharing and the like. It was best expressed in my mind by Nancy Savage who testified. She is head of that Agents Association. She testified at appropriations last year.

On the issue, she said, the FBI culture is one of hard work, dedication to the citizens of this country and excellence in its endeavors, which I think is the best I have heard in terms of FBI describing the FBI culture.

Now, let me start from distinguishing between collection and the analysis. I would be the first to concede that we have not done a good job in analysis. We have not had either the technology nor the analytical cadre of individuals that we have needed to do the analysis which you are describing. I am not certain that a separate agency would satisfy that. In fact, I think it would institutionalize that which we are trying to prevent—that is, compartmentalization.

Because I absolutely believe that the analytical cadre that is looking at the facts ought to have the tasking ability, ought to have integration with the tactical analysts as well as the agents so that they become familiar with the information that they are getting and digesting and upon which they are doing the analytical piece.

If you look at the FBI and what the FBI is good at, an FBI agent is good at doing investigations, and those investigations can be in counterintelligence. We have done those for a number of years, where you run a counterintelligence investigation in trying to determine what attack the Russians or some other country is trying to make on our infrastructure.

Senator THOMPSON. This is a different deal. We know now that we are dealing with a different kind of enemy that lies there perhaps for years secretly planning, that we have not been able to necessarily infiltrate very much. Isn't that a different situation we are facing?

Director MUELLER. You are looking at it from the intelligence point of view. And how do you expand on your knowledge of the person? You don't arrest them right away, because you want to find out who else is in this network, turn them against each other. That is something that we have been doing for a number of years. But, as collectors, the FBI agents are the finest collectors of intelligence in the world.

Now one of the things that we have to do, and I think is changing since September 11, is for agents who are very good in the criminal sphere to look at a piece of information and not run it through the sifting that you do to determine whether it would be admissible in court. In other words, is it hearsay? Well, I am going to thrust it aside. Do I have lack of foundation? Therefore, I am going to disregard that. And we are changing to have everyone in the organization understand that a piece of information is a piece of information that has to be put into a matrix and looked at as a whole.

But in terms of the collection, I don't think there are any better around; and to set up another institution to do collection with the United States is fraught with difficulties in my mind. You then would have another institution that is developing sources in the community and sources that may provide information on terrorist matters may be involved in criminal enterprises, whether it be narcotics or food stamp fraud, which we have found, and you will be divorcing those collection pieces from each other and again stovepiping it.

The use of technical resources where you are doing interceptions and the like, I have heard stories—not good stories, not necessarily horror stories—about other countries that have this dual setup, where there has been the failure to pass off in the Intelligence Community to the law enforcement community that has resulted in disasters in terms of being able to prevent attacks.

One other thing that I would mention just for a second. That is, it is important in this day and age that we be integrated with our counterparts overseas. In every country I visited, Middle East, Southeast Asia, there is—our counterpart will be either a primary law enforcement counterpart or an intelligence counterpart with whom George will have the discussions. But it is important as we proceed and gather the intelligence that we develop these relationships with our counterparts overseas. We have developed through our legats—our expanded legats—those associations that enable us to get intelligence from our law enforcement components.

If there is a separate entity in the United States, we will be lacking and missing, I believe, the benefit of all of those contacts that we develop in the law enforcement community around the world to supplement what George has in the Intelligence Community.

Senator THOMPSON. I take your point, Mr. Mueller.

I am impinging on others' time. I apologize to the Chairman and my colleagues. That is my questions.

Chairman GRAHAM. Thank you, Senator Thompson.

Ms. HARMAN. Thank you, Mr. Chairman. It has been a long day for the witnesses and for others here who also have questions, so I am going to try to stick within my time limits.

As I was sitting here, it occurs to me that over a quarter of a century ago I was chief counsel and staff director of a Senate Judiciary subcommittee. At that time, there were very few women in staff positions on subcommittees. I think, if memory serves, there were no women Members of the United States Senate. There was a very able Senate staffer named Fred Thompson who was extremely well known at the time—in the Watergate investigation.

But the things that we did were hard, but I don't think any of them as hard as pulling together all the facts that relate to the plot of 9/11. And I just want to say as a matter of personal pride, as I sit here with Senator Feinstein and Congresswoman Pelosi watching Eleanor Hill perform, that this moment is a long time in coming, and I just commend her for her talent and dedication and for the amount of work she's been able to pull together for those of us who are part of this joint inquiry, and in an elegant and reasonably excellent fashion. I am very proud of the work that you do, Eleanor.

The purpose of this joint inquiry, as I have said many times, and many others have said also, is to look backward for the purpose of looking forward to bridge the gaps in intelligence capabilities and prevent the next attack. I am not as interested in the failures that happened pre-9/11 as I am interested in protecting, preventing—not having failures at a future time when we may be attacked again.

That future time, according to Director Tenet—and I strongly agree—could be in the next hour, tomorrow morning, tonight. The sniper incidents in Washington show us how vulnerable we are to attack and so do the recent events in Bali, Kuwait, and elsewhere. At any rate, the thrust of my quest is to go forward.

Let me also add, as Senator Thompson did, that some of what needs to get done does not need to get done by the people at the witness table. It needs to get done by Congress. I think it is tragic that our fiscal year 2003 intelligence authorization bill has not been acted upon. It's held up because of a dispute about the precise powers of an independent commission. Those precise powers should have been agreed on long ago. Everyone supports the commission.

And what's being held up in addition to the commission is an information-sharing bill that passed the House 422 to 2 and has been introduced in the Senate, funding for a wide variety of things, some of which are classified and some of which are public. That bill should be law.

The same goes for the Homeland Security Department legislation which we've all been discussing. Director Tenet talks about the back end. That bill is the back end. It's also some part of the front end because it would create an intelligence fusion center so that we get better at giving real-time information about the nature of threats to our first responders. If we don't get better about doing that, we're going to continue to be vulnerable.

So, I could go on about what we haven't done. Those are two big things that we haven't done.

And yesterday a bipartisan group from the House that were the original authors of the homeland security legislation held a press conference where we said it's time for the Senate to act to vote its will on whatever version of civil service the Senate wants to pass, and then for a conference to occur, the White House to buy in, and for us to get a bill signed. And I strongly believe that's true.

But what I want to focus on for a few minutes today are things that are within your power, you, the witnesses before us, to fix. And, again, I'm not interested in why they were broken. I'm interested in how they get fixed. I think the fair question—and you can't answer it the way I'm going to put it, but you can answer it

as I break it into parts—is this one: On 9/11, 19 hijackers boarded four planes at Logan, Dulles, and Newark and crashed them into the World Trade Center, the Pentagon, and a field in western Pennsylvania. Can those attacks—would those attacks be prevented today?

Now, of course, you can't say yes or no, but what I'm going to ask you is probabilities. I want to know, based on all the things that you are fixing—and you documented them very carefully—what is the probability? How much improved is it over where you were on 9/11 that you could stop not necessarily those precise attacks, but major attacks targeted at the U.S. homeland. How much better are you at doing this than you were pre-9/11?

And I'd like to ask General Hayden as well. General Hayden.

General HAYDEN. Thank you, ma'am. A couple of things have changed. And one thing fundamentally has changed. Let me begin with some of the perhaps less-impactful changes. One is additional resources, and that's been very important. The committees here have given additional monies that have been asked for by the President and some additional manpower. That helps a lot.

You heard my reference earlier about transformation and chasing modern signals. That's good. We've also, the three of us and some others not at the table, have improved procedures largely in the area of how quickly and agilely we share information. That's also been very valuable and has an impact.

Now, let me tell you what I think the most impactful thing has been. And much has been made about the DCI's declaration of war against al-Qa'ida in October of 98 and what did we do about it and what difference did it make and so on. Let me tell you a fundamental lesson I've learned. There's a big difference between George declaring war on al-Qa'ida and America declaring war on al-Qa'ida. The most fundamental difference between today and the circumstances that we existed under on the morning of the 11—I used this metaphor before in closed session. Let me quickly review it.

Prior to September 11, the model of your Intelligence Community was playing American football with the opposition on the 2-yard line, and it was forever first and goal. They would run a play and our measure of merit would be if we stopped them from getting into the end zone on that particular play. And if we did, some metaphorical official would take the ball, put it back on the 2-yard line and declare it to be first and 10 again.

What has changed is that we are delaying, denying, disrupting, and destroying portions of the al-Qa'ida network. Prior to September 11, time was infinite for them. It was always on their side. They could take whatever systems they needed to take in order to be secure. They can no longer do that. Things are going bump in their night now, and that puts us at a great advantage. That's the big difference.

Ms. HARMAN. Thank you.

Time is short so I just would like just a very short answer from Director Tenet and Director Mueller, because I want to turn to something else. Probability: How much better are we?

Director TENET. You're a lot better at probability. You're a lot better. One, every morning there's a common-threat matrix where law enforcement and intelligence data comes together in one place

with actions that have been assigned and everybody sees it. And it's disseminated broadly. Number two, some of the old classification rules have gone out the door—Orcon controls on HUMINT, controls on his raw traffic, controls on his criminal files. Because of the PATRIOT Act, all of that is moving to people quicker than it has before. There's a speed with which this is all happening in terms of the hand-off between the disciplines. There's a greater awareness of what's going on in the country.

I can't give you probabilities. Is it better than it was a year ago? It's a heck of a lot better. And I believe Governor Ridge has done a good job in his role in terms of trying to bring this process together. So, yes, we're better. Can I give you a guarantee? Absolutely not.

Ms. HARMAN. Okay. Thank you. Director Mueller.

Director MUELLER. At the FBI there are four things, I'd say, areas in which we are substantially better:

One, the shift in mission. I think there isn't an FBI employee—not just agents—out there who doesn't understand the necessity of pulling together of pieces of information, and, regardless of how innocuous they may seem, making certain that they are written up and pursued.

Secondly, the joint terrorism task forces in all the 56 offices. That has greatly expanded our capabilities, not only by having additional agents assigned to counterterrorism, but by leveraging that with the assistance of the State locals and providing a mechanism for information to come from State and local as well as information going back to State and locals.

Thirdly, in personnel. We have hired a number of over—over 100 analysts and what we call IOSs, and another 143 of IRSs. Half of them, approximately, in both categories, are still in the background process, but the others are onboard and are doing that type of analysis. In terms of agents, we're putting 900 new agents through the Academy and we've reassigned approximately 500 to counterterrorism.

And lastly, technology. Within the next—one of the deficiencies we had in exchange of information was not having a Top Secret SCI network upon which we could shove or push to the analysts those classified documents and cables that we get from others outside as well as within our building, and we have put together a plan that is going to enable us to do that, and within the next 30 days it will go up, so it will complement the analytical capability we have in the form of analysts by giving them in the basis for the sharing of the information within the organization as well as between us and the CIA.

Ms. HARMAN. So probability is what?

Director MUELLER. All I can tell you is we have, I think, certainly doubled our capability since last year, if not trebled.

Ms. HARMAN. Okay. New question. Senator Levin detailed the plot in his charts and talked about failures, most of which related to watchlisting. My first information about that came from a Newsweek article, June 10, 2002, which carefully documents this material as well. I'm not sure why I learned it from Newsweek first, but at any rate that's where I learned it.

My specific question is watchlist. Director Tenet, in your testimony on page 18, you detail all the changes you have made. What I think we need to know, briefly, is how will the new—and you deserve a sandwich. As one of the mothers on this committee, I think you deserve a sandwich. How will the new watchlist system work? Will it pick up all the stuff we need it to pick up? Will it be one watchlist? I assume it will be, based on the TIPOFF State Department system. Will it be run through a national watchlist center or this terrorist identification classification system that Senators Feinstein and Wyden are proposing? Who will run it? Who will ensure that the information gets inputted? Who will have access to it? How will you make certain that the airlines are paying attention to this, or the trains or—you know, pick any number of things.

I think the American people need to know not just that the watchlist is being fixed, but precisely how it is going to be fixed; how it is going to be funded; how it won't disappoint us next time. And I don't know whether you can answer that question here, but I think it's very important for the combination of you, specifically the FBI and the CIA and maybe other agencies, but at least you since you're the witnesses, to provide this committee specific information about what is changing, and, better yet, what has already changed so that people who happen to be at strange meetings in Malaysia definitely get watchlisted when the first person who notices this notices it.

Director TENET. And I will do that with some detail for you, Ms. Harman.

Ms. HARMAN. Okay.

Director MUELLER. I would say that it is being worked on by Homeland Security. It's yet another reason why the Homeland Security Department would be helpful. And I will say I think both organizations have changed their procedures with regard to watchlists, consolidating in one—we have in the FBI consolidated in one unit the information that goes into TIPS or the TIPOFF system.

We have established our own watchlist that is tied into NCIC, which is a subcompartment of NCIC. And the importance is not only having a consolidated watchlist, but also reviewing that watchlist to make certain that persons get off of it when they have been run through a system and come out clean.

So individually I think both of our institutions have changed their procedures to make certain that what happened before, prior to September 11, does not happen again. But it still does not totally satisfy the necessity for having one location within the Federal Government to address that.

Ms. HARMAN. You remind me, Director Tenet, of my favorite rant about e-mail. You push the button and you think people are supposed to know something and act on it, and sometimes they don't. The watchlist cannot become a push-the-button exercise. It has to be an active interactive exercise so that consequences flow from listing names.

Last question. There's one member of the Tenet family who knows how to fix things. This is called "Dare to Repair." I trust that—written by Stephanie Glakas Tenet, who is the repair person in the Tenet family. But I'm hoping——

Director TENET. She's fixing the watchlist system.

Ms. HARMAN. Well, that makes me—you know, if you want to get the job done, put a woman in charge. So that makes me very happy.

Director TENET. She's clearly in charge.

Ms. HARMAN. I believe that. At any rate, this is an introduction to my last question, which is the many people in your agencies who have been trying to fix things, the heroes and heroines pre-9/11 and post 9/11, not the big shots, the little shots who have been doing extraordinary work, I have said from the beginning, again, that we had good people with inadequate tools. And I would like each of you to tell us one story about somebody that we won't know who had it right pre-9/11 and continues to do extraordinary work on behalf of the American people, because I think that is a message that doesn't get out enough. General Hayden.

General HAYDEN. I'd point to the folks, ma'am, in our counterterrorism shop, particularly those who are analyst linguists who have been working this problem for decades. The Army has a phrase, "It takes 18 years to grow a battalion commander." It takes about that long for us to grow someone so knowledgeable about this target that it can take the language and the Koranic references and the indirection and the obscure in the conversation and turn into something very useful for American intelligence. That's a life's work. You don't get that off the street.

Those are the folks that have looked at this, who looked on the scene of the morning of the 11 that I referred to earlier—not that they were responsible, but that they had a sense of responsibility. And that's why we had to tell them, "It's all right, get back to work." I'd single out those folks.

Ms. HARMAN. Director Tenet.

Director TENET. Well, Ms. Harman, I'm going to come back to this woman in the middle of the watchlist, who's one of the finest employees that we've ever had employed out there, who starts her days early in the morning, sifts through hundreds of cables, passes operational leads, is as vehemently opposed to these people who are trying to kill us as anybody you've ever met in her life. She's a real hero in this story. And the notion that I'm going to take her out and shoot her is about the most ridiculous thing I've ever heard because of her passion and commitment to her job, and I don't want her for a minute to believe that I'm going to come after her or somebody's going to come after her because we overwhelmed her and didn't give her all the tools she needed. I mean, I'd like you all to meet her sometime.

Ms. HARMAN. But you're going to give her better tools now, right?

Director TENET. Yes, ma'am.

Ms. HARMAN. And then she'll be accountable for a job that is a different job from the one she was asked to perform before.

Director TENET. I want to talk about the—accountability is always important. But we also need to be careful. There are people who are taking enormous risk, working at enormous pace. And we've all talked about risk aversion. We've all talked about what people will or will not do, you know. So let's be careful, because none of these people believed that they were doing anything but the best job they knew how to do. There was no intent to withhold

information. There was no intent to lie, cheat, or steal. They did everything they knew how to do and it wasn't flawless.

You know, if anybody's going to take responsibility, I take responsibility.

Ms. HARMAN. Well, I appreciate that. And that's part of leadership is taking responsibility. But I also think, in line with some of Senator Levin's comments, that we need to give people good job descriptions, good tools, and then make certain that not just they try hard—which I am always for—but that they succeed in what I think is the most important endeavor that people are engaged in in the Federal Government.

Director Tenet.

Director MUELLER. I would pick the analyst also for the FBI who provided the following description of her day to me. She said, imagine for a moment that you have been given a jigsaw puzzle in a plain box. Inside are thousands of pieces varying slightly in shape and color, but none give any indication of the picture that is to be formed from them. You have no picture on the box and do not know what the puzzle is supposed to look like. You're aware that the majority of the pieces don't even belong to this puzzle. But you are cautious in discarding pieces which could belong. The ones that do belong are not enough to complete the puzzle or even give more than a hint of the picture that they are meant to form.

Now, imagine that this is not a game, but a matter of life and death, where every threat could be real, every speculation could have merit, every source report could stop an attack. In your 12-, 14-, 16-hour workday, try to determine which pieces belong to the puzzle and where they fit. What does the picture look like? Who are the players? What are the patterns? What are we missing? And how do we find it?

Now try doing this with insufficient personnel and technology. Which comes to your point, is we have to give them the personnel and the technology. You are overwhelmed with information, overburdened by caseloads, stymied by technology, and constrained by laws and policies. And you try to supplant resources with longer hours, missing more time with family and friends, celebrating yet another holiday season a day or a week late or not at all. All of this is done knowing that, despite your commitment and your determination, the pieces simply may not be there for you to put together. It is done knowing that lives could be lost in one day, and you watch in horror when your fellow American—as your worst nightmare is recognized.

Ms. HARMAN. Mr. Chairman, I thank the hardworking employees of these agencies, and I wish them well, and tell them that they have the security of America on their shoulders. And I wish even better wisdom for the people who have appeared before us today and thank them for their testimony. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you very much, Congresswoman Harman. And this completes the designated questioners.

The order for five-minute questions will be Graham, Goss, Shelby, Pelosi, DeWine, Hoekstra, Peterson, Bereuter, Roemer, Lugar, Reyes, Wyden, Boswell, Gibbons, Feinstein, Hatch, Bayh, Roberts, Kyl, Condit.

On October 7, over Mr. Tenet's signature, the CIA issued a declassification of certain information that had been previously contained in a National Intelligence Estimate. I'm going to read two paragraphs from that declassification:

"Should Saddam conclude that a U.S.-led attack could no longer be deterred, he probably would become much less constrained in adopting terrorist actions.

"Such terrorism might involve conventional means, as with Iraq's unsuccessful attempt at a terrorist offensive in 1991, or chemical and biological weapons. Saddam might decide that the extreme step of assisting Islamic terrorists in conducting a weapons-of-mass-destruction attack against the United States would be his last chance to exact vengeance by taking a large number of victims with him."

From what I read and speculate, there is a prospect that we might be under way with U.S.-led attacks which Saddam Hussein could no longer deter, within the next 100 days. In that time frame, I want to talk about where we are defensively and offensively in protecting the people of the United States especially here in our homeland.

First, on the defense, Director Mueller, what would you describe as our state of preparedness to deal with the embedded international terrorists who are within the United States, similar to the 19 who hijacked the airplanes on September 11, and how would you describe the acceleration of pace of attempting to identify the location, the scale, the skills, the nature of support and command and control for those terrorists who are living among us?

Director MUELLER. I don't have the figures in front of me, but I can tell you that since September 11 the number of investigations that we have undertaken has doubled if not tripled. The number of interceptions we've sought approval from the court for has at least quadrupled, if not more. The reallocation of or the reassignment of 500 agents to counterterrorism has substantially assisted in our ability to enhance our coverage of individuals in the country who would do us harm.

I will tell you also that with the issue of Iraq there, we have—and without in open hearing giving too much detail—focused on that possibility and are increasing our resources addressed to that particular—addressed to those individuals who might be in our country that might find this as an occasion to commit some sort of act were we to initiate some operation with regard to Iraq.

Chairman GRAHAM. If you could summarize, what do you think should be the level of assurance that the people of the United States would have that we would be successful in defending them against this probability that Saddam Hussein would be much less constrained in adopting terrorist activities?

Director MUELLER. Well, I think we are doing—we are looking at every lead. We are looking at every possibility that comes to our attention of terrorist—not just terrorists who may be associated in one way, directly or in directly with Iraq, but others who might use this as an occasion to exploit the opportunity to undertake an attack.

I have a hard time—I have a hard time telling the country that you should be comfortable that we've covered all of the bases in the

wake of what we saw they were able to accomplish on September 11. I mean, that was a watershed in terms of the accomplishment of a group of individuals to come together utilizing modern means of technology, in terms of their communications, their planning, their organization, their travels, a type of discipline that prior to that time I don't think we had seen.

And so I am uncomfortable sitting here saying, look, we are taking every step, but based on the fact that we are taking every step, you, the American public, should not be aware that there is a substantial risk out there that they could undertake—and by "they" I mean not just those associated with Iraq, but those associated with al-Qa'ida or Hizbollah or somebody else. But I would be uncomfortable in saying that you should relax and say the FBI is taking care or the FBI or the CIA is taking care of that issue.

Chairman GRAHAM. My next round, I'd like to go to the offensive and ask some questions of General Hayden and Director Tenet as to what we're doing over there against these terrorist groups. Congressman Goss.

Chairman GOSS. Thank you, Mr. Chairman. Director Tenet, how long have you been the DCI?

Director TENET. Five years and a few months, sir.

Chairman GOSS. That gives you longevity on the panel, then, of time held in the job; is that correct?

Director TENET. I believe so; yes, sir.

Chairman GOSS. How many DCIs were there immediately preceding you in the period of the nineties?

Director TENET. I believe it was four in a period of 7 years.

Chairman GOSS. Four in a period of 7 years. So we have five DCIs, and you've had 50 percent of it, during the decade of the nineties; is that about right?

Director TENET. There's actually four in the nineties. Four DCIs in the nineties.

Chairman GOSS. A lot of change going on. Some of those previous DCIs said that they didn't have much access to the White House. I think some recall a joke about—now a bad joke, but a joke at the time about a small plane that crashed near the White House as the Director of the DCI was trying to get in to see the President. Do you remember that story going around?

My question goes to this. You made a comment about the seriousness of this war. You certainly made it clear to the oversight committees. I don't think there's any mystery in the oversight committees, those of us who were also here during the longevity of your tenure, about this problem. There's really not a whole lot new that's come out of this for those folks who have been focused on it.

My question that has haunted me, and I imagine has haunted you, is how come nobody listened in '98 at the right level? Why didn't we get out of OMB, why did not we get out of the people who were making the decisions on awareness, that we needed to reinvest, that we were dangerously underinvested, that we were letting capabilities slide, that our technology was falling behind? It was clear.

I'd love to have your answer. And I would be very happy to have Director Mueller's and General Hayden's as well. But I'm not sure Director Mueller had been there long enough.

Director TENET. Look, sir, I can't speak to what the reaction was to our requests. I think that, you know, you really have to talk to the people who were making judgments on what we were asking for. I think that this is an endeavor where if you don't make the investments, you know, you can't function at the level you need to function at. I think we made that case as compellingly as we possibly could, and I believe that, you know, whether there was a deficit that was at stake, whether there were budget caps that were at stake, whatever the reasoning was, whatever the—we just needed more support than we received.

Chairman GOSS. What's the primary function of the Federal Government? It is national security, isn't it—to guarantee the safety and well-being liberty of the United States of America. Shouldn't that be job one? And shouldn't the leaders be listening? Okay.

My second question, then, General Hayden, you said something about bin Ladin coming across the bridge—hypothetically, of course. But I take that to mean that if bin Ladin did come, there would be capabilities that we have that we can use elsewhere in the world that we cannot use in the United States of America; is that correct?

General HAYDEN. Not so much capabilities, but how agilely we could apply those capabilities. A person inside the United States becomes a U.S. person under the definition provided by the FISA Act.

Chairman GOSS. Special protections, according to your testimony.

General HAYDEN. And special protections then apply. There are procedural steps that one can identify such a person as the agent of a foreign power, but one's got to go through those procedural steps. Now, take that metaphor and apply it to somebody without the persona of Usama bin Ladin, and you can see the challenge of trying to cover people inside U.S. borders, even if they will us harm.

Chairman GOSS. Well, again I don't want to get into details. I'm aware of the public nature of this meeting. But let's just suppose this sniper is somebody we wanted to catch very badly. Could we apply all our technologies and all our capabilities and all our know-how against that person, or would that person be considered to have protection as an American citizen?

General HAYDEN. It would—that person would have protections as what the law defines as a U.S. person, and I would have no authorities to pursue him.

Chairman GOSS. So the answer is that person has some protections just by being in the United States of America, and if that act were actually taking place overseas, we would be able to bring more to bear to deal with it.

General HAYDEN. Absolutely.

Chairman GOSS. That's a fair statement?

General HAYDEN. Yes, sir.

Chairman GOSS. Thank you. I'm not sure everybody in this country understands just how many safeguards we have for American liberties, and I think it is very important to underscore that. There is a price for it. And we are trying to find the balance and what that price is, and I appreciate your answer to the question.

Finally, Director Tenet, you didn't seem satisfied with the amount of time you had to answer a question of some dispute about a matter in New York. Would you care to use the time to elaborate?

Director TENET. Not at this moment, sir. I think that there is a—we have a different view of what happened there. But let's work through that.

Chairman GOSS. Well, for your comfort zone, let me tell you that I think that we do understand that there are two stories. When you put it all together, it does make some sense to what different people who were doing their job responsibly thought, and I don't find an inconsistency in it.

The last question—which I will not ask, because my time has expired. Thank you.

Chairman GRAHAM. Thank you, Congressman. Senator Shelby.

Vice Chairman SHELBY. Thank you, Mr. Chairman.

Director Tenet, I'm going to refer you to I believe it's page 25 of your written statement that's been made part of the record today, and I wanted to quote—I believe it's paragraph 3 from it. Page 25, paragraph 3. I believe it's the second sentence. "When we realized surging wasn't sufficient, we began a sustained drumbeat both within the Administration and here on the Hill that we had to have more people and money devoted to this fight."

Did the drumbeat begin in '98, or before?

Director TENET. I have to go back and look at my records, sir.

Vice Chairman SHELBY. Okay.

Director TENET. But I believe it did, at least internally, in terms of what we were requesting. But I'll check that for you.

Vice Chairman SHELBY. I want to go back to part of that. This is not classified, but this was in the appropriations hearing in '98, and the question to you and directed to you and Director Freeh at that time was about funding. And I'll leave out Director Freeh's at the moment.

He's talking about counterterrorism support. And then I'll—and I believe it was Senator Arlen Specter, former chairman of this committee, was asking the question, and he was talking about resources.

And quoting you, you say, "Senator," responding to Senator Specter, "I would like to respond and just say I think we're already at war. We've been on a war footing for a number of years now. I do not think it's a question of money in our case. I think it's a question of focus, operational tempo, the aggressiveness with which we pursue this target. I do not have any doubt about the level of that effort today, and I would challenge your premise about the lack of human intelligence against the terrorist target. I think it's something we should talk about behind closed doors, because I think that effort is better than it has ever been and growing. I think there are successes to prove it, and some of the facts we've laid down in open session."

But what I—my point is you were saying, as we understood it in the context—I was in that appropriation hearing, being an appropriator—that it was more than just money; it was a question of focus, operational tempo, the aggressiveness with which we pursue these targets. These are your words.

Director TENET. Right. I believe we had all those things.

Vice Chairman SHELBY. Do you disagree with that, your statement in 1998 before the Appropriations Committee?

Director TENET. Was it after the Africa bombing, sir? Do you know when it was?

Vice Chairman SHELBY. It was after. It must have been after.

Director TENET. I'd also say that in roughly the same time period, you can go look at it for your record.

Vice Chairman SHELBY. Yes.

Director TENET. Senator Kyl asked me a question in closed session about how much money we more needed for the community each year every year and I said between nine hundred and a billion dollars in closed session for the years that followed I think that was in 1998 too.

Vice Chairman SHELBY. And, Director Mueller, you were not there on this occasion. You were not the director. But I'll read this into the record. And this same question was asked, basic question by Senator Specter at the appropriations panel to Director Freeh. And Director Freeh—and I'll quote him from the record—responded as follows: "Senator," speaking of Senator Specter's question, "first of all, I appreciate all your remarks and your support, particularly in the counterterrorism area which goes back many, many years. We've grown in three years from a $93 million budget to a $243 million budget in counterterrorism. You and your colleagues were generous enough last year to give the FBI, I believe it's 1,264 new positions. We are hiring these people. We are training them. We're putting together both the human resources and the infrastructure to support the counterterrorism effort. We are in two or three times better condition in '97 than we were in '93 to undertake our counterterrorism mission, a mission which as you point out is a huge and growing one. We are in Saudi Arabia. We're taking fugitives back from Pakistan. We are in many, many places where we have not been, which is why we need our legats. We're doing everything we can right now to absorb this vast increase in resources."

This is the Bureau, your predecessor: "I would rather absorb that growth before we start another huge influx of resources."

I don't know if, Director Mueller—and I am going to say, again, you were not there. You were not the director. But you ought to familiarize yourself with this. I'll furnish you a copy of it. My time's up. I await another round.

Chairman GRAHAM. Thank you, Senator.

Congresswoman Pelosi.

Ms. PELOSI. Thank you very much, Mr. Chairman. Again, to our distinguished witnesses, thank you for your testimony today, for your service to our country. I associate myself with the remarks of Congresswoman Harman commending the people, the brave young men and women and not so young men and women who work with all of you every day to protect our country. We are grateful for their courage and their patriotism.

I just want to throw out to the three of you some observations that I have for your comment. When we first went into this inquiry and in the aftermath of 9/11, it appeared that the hijackers were people who came to the United States, lived in isolation, as the Director has described, were not conspicuous, didn't break any laws,

et cetera, and that at a certain moment a button was pushed, the message went out, and they went into operation.

In the course of the hearings and our reading and the rest, it appears that maybe they weren't living lives of such isolation and that they might have received comfort and support, witting or unwitting, from some people in our country—A.

B—especially from Director Tenet's testimony this morning, I would observe that when we ask the question, could this have been avoided, I'm becoming more discouraged about that as I hear more testimony, because it appears that if this wave of hijackers for some reason or other would have been apprehended, there may have been another tier to replace them. I don't necessarily mean a whole tier, just people to fill in different slots.

And so this was so well orchestrated that—and I don't want this to sound hopeless—that they had people to fill in if somebody got more than a parking ticket; or we knew of the people who met in southeast Asia, we knew of that meeting, and then we identified and somebody was on the watchlist, that that might have been a window on their activity, that might have broken this. But it may not necessarily have prevented somebody from being in the wrong place at the wrong time in terms of the security of the American people. I just throw those observations out. Was there more here than meets the eye in terms of the support system for these hijackers?

And I would just add a third observation. And that is, I've always thought that the apprehension of Moussaoui and the timing of 9/11 may not have been the natural course of events, that Moussaoui's arrest may have triggered the hijackers into going into action. Now, when I have asked this question in the past in hearings, people say, oh, this hijacking was planned years in advance. It may well have been. But that still doesn't mean that the timing might not have been accelerated when the window on their activity was opened by the apprehension of Moussaoui. I put that out there for your comments. Thank you.

Director MUELLER. Well, I'll address the support within the United States. I think a critical distinction that you identified is witting versus unwitting. I do believe, and we have seen a number of instances they were provided identification, some sort of support by persons they come in contact with in the United States, but these are unwitting individuals. Some of them have been arrested and prosecuted for that support—for instance, providing identification to one or more of the hijackers.

And so, yes, I think there were unwitting supporters within the United States, and that's an important distinction to recognize.

As to whether or not—as to the issue of are there others out there who would have filled the holes had there been holes, I think the answer to that has to be yes. I mean we all know that in the camps in Afghanistan approximately 10,000 individuals went through the training and are now dispersed throughout the world. We also had at least two individuals who attempted to get into the United States who we know to have been individuals who were knowledgeable, and, we believe, part of the plot, who were part of the cell in Hamburg, Germany, who tried to get in, but their visas

were denied and they accordingly could not be amongst the hijackers on September 11.

So, yes, there are many others out there, I believe—and I think George would have his own views—who would have been able to fill those slots should the need have arisen.

As to the last point you make in terms of the—whether or not the arrest of Moussaoui might have triggered the date or determined the date, I'll leave that up to George. One of the problems we have is I can't get too much into the events surrounding Mr. Moussaoui because he is facing trial in Virginia this summer.

Ms. PELOSI. Thank you, Mr. Director. Mr. Director.

Director TENET. Ms. Pelosi, I think you know with regard to your first points, the director—you know, Binalshibh tried to get into the United States. Visa denied. Somebody else came in. Hazmi and Mihdhar took flight training, didn't do well at it. Hani Hanjour came in and became a pilot. On we go.

With regard to Moussaoui, assuming that I'm allowed to talk to Moussaoui, the one thing that I notice is nine days after he's arrested everybody starts buying their tickets. So, yes, these are well planned. Or 11 days. Yes, these are well-planned events, but they are determined by the operational security of the environment at the time.

Now, why it happened that they started buying their tickets so soon after his arrest I don't actually understand, but you have to pay attention to it. And so they react and they're resilient and they make decisions based on their own sense of operational security.

Ms. PELOSI. Thank you, Mr. Director.

General, did you have any observation you would like to make?

General HAYDEN. No, ma'am, it is very hard for us to comment. The core of the question is so much domestic that we have very little to add.

Ms. PELOSI. Thank you, General.

I just want to make one observation, Mr. Chairman, because I know my time is up. I direct all of us to page 20 of Director Tenet's testimony, and on that page you are quoting the National Intelligence Estimate of 1995. And in it you say:

"Our review of the evidence obtained thus far about the plot uncovered in Manila in early 1995 suggests that the conspirators were guided in their selection of method and venue of attack by carefully studying security procedures in place in the region. If terrorists operating in this country are similarly methodical, they will identify serious vulnerabilities in the security system for domestic flights."

I point that out because I think that in looking into the causes of 9/11 and assessing the performance of agencies with the responsibility to protect the American people from terrorist attacks, we focused very much on our Intelligence Community. But I do think that a statement of that kind points to a broader area, to broader areas of responsibility. And there are other statements in all of your testimony that speak to where we are—where we have exposure, they will exploit it.

Again, on an earlier page in the testimony: A sign that our warnings were being heard both from our analysts and from our raw in-

telligence we disseminated was that the FAA issued two alerts to air carriers in the summer of 2001.

I think that we will have an excellent product in our report of this committee. I think once again it points to the need for an independent commission to review a broader range of agencies with the responsibility, because you can have the best intelligence-gathering, you can all share the information, General, you can do whatever you do that you can't talk about, and you don't do it in this country, but the fact is there is a great deal else where we have exposure, and it seems that part of their modus operandi is to exploit the vulnerabilities, the security weaknesses that they may see.

So with that, Mr. Chairman, I once again thank the gentlemen for their distinguished service and yield back the balance of my time.

Chairman GRAHAM. Thank you, Congresswoman Pelosi.

The next is going to be Senator DeWine, and after Senator DeWine has asked his questions I'm going to call for a five-minute recess. Senator DeWine.

Senator DEWINE. Thank you, Mr. Chairman.

General Hayden, I thought the discussion that you had with Congressman Goss in regard to your powers or lack of powers with regard to the snipers was very instructive. And it is, as you point out in your testimony, the type of discussion that we should be having.

You say in your testimony, and I'll quote: "I'm not really helped by being reminded that I need more Arabic linguists or by someone second-guessing obscure intercepts sitting in our files that may make more sense today than it did two years ago. What I really need you to do is to talk to your constituents and find out where the American people want that line between security and liberty to be."

I don't disagree with that statement, but I think I would take it a little further. I think that we as a Congress, specifically this committee, these committees, have an obligation to do that. But I also think you have an obligation to do that. We write the laws. You, or your lawyers, then interpret them. And you issue very long regulations, and I won't bore anybody by reading some of these regulations, but they're long and they're extensive.

And then you take that down and you take—those lawyers create the regulations or rules and you take them down and—with manuals down to the people in the field who you ask to actually make these decisions every single day.

And so I think you have an obligation, candidly, to come back to us and to say, Senator, do you really want to do this? Do you understand what we're not doing? Do you understand who we can't target? Do you understand what information we can't get? And I think that you have an obligation to do that as often as you can.

Now, I will say that your comment that you made, public testimony about bin Ladin crossing the border between Canada and the United States, you did that. And I think you're right. You apparently didn't hear much complaint from Congress. So I will certainly give you that. But I would just say that I think we all have an obligation to do that. As I've discussed with you and as I've discussed with some of your team, I'm not sure you're totally interpreting the

law correctly. But that's something that we should be going back and forth on, and something that should be discussed and discussed. And so I would just make that comment.

Mr. Mueller, you made a comment in regard to continuing resolutions and the problem connected with that. You say a long-term—my emphasis, but I think it's what you meant—a long-term continuing resolution could have a significant impact on our analytical program.

Now, let me ask all three of you if you could comment about the consequences of long-term continuing resolutions, particularly this year, but anytime that you might get one, what it might entail. And we will assume that means basically flat funding.

General HAYDEN. I'll go first, Senator.

Senator DEWINE. I think that's something we need to know and need to get out.

General HAYDEN. Well, fundamentally with a continuing resolution, we're prohibited from having new starts—and I've tried to emphasize in my testimony this is all about newness, this is all about transformation, this is all about chasing a global telecommunications revolution.

To put us through some portion of the next fiscal year without any new starts, without any ability to pivot left or right but just to continue straight ahead, that penalizes us.

Senator DEWINE. Thank you. Director.

Director TENET. I agree with Director Hayden.

Director MUELLER. And also the delay in bringing on additional analysts, as I pointed out, additional agents and, for us, also support personnel. Those delays mean, you know, that just—that much longer before we get those individuals onboard, that we need to get the job done right.

Senator DEWINE. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Senator DeWine.

At this point we'll take a five-minute break, and Congressman Hoekstra will be the first questioner when we reconvene.

[Recess.]

Chairman GRAHAM. Call the meeting to order. The panelists could reassume their seats. I will repeat the order in which questioners will be called upon. After Congressman Hoekstra, it will be Mr. Peterson, Mr. Bereuter, Mr. Roemer, Senator Lugar, Mr. Reyes, Senator Wyden, Mr. Boswell, Mr. Gibbons, Senator Feinstein, Senator Hatch, Senator Bayh, Senator Roberts, Senator Kyl, Mr. Condit.

Now, we just need our panelists.

Gentlemen, I want to thank you very much. I know this has been a long day for you and also the preparation that went into today. So I thank you for your candid and very informative responses.

Congressman Hoekstra.

Mr. HOEKSTRA. Thank you, Mr. Chairman, and thanks to the panelists for being here for a very informative hearing. I think from Eleanor Hill's opening statement at the end of that opening statement there are a lot of questions that were raised that I hope this committee considers and we take a serious look at.

I want to focus on the comprehensive strategic plan. There is some question as to whether one of those existed prior to Sep-

tember 11. A Department of Justice inspector general report recently said the FBI has never performed a comprehensive written assessment of the risks of the terrorist threat facing the United States. A national intelligence estimate of the al-Qa'ida threat overseas was not done prior to September 11.

The question that I have is, is there now a comprehensive strategy document or plan in place that each of the three of you have had input into that you would agree on that this is a strategic plan, these are the roles that each of our organizations and agency plays, what are its fundamental components, and then, as you're talking about the fundamental components, there has been a lot of discussion about, you know, people who can get into the country and people who cannot, the integrity of our visa system and our border controls.

Does the strategic plan address the issue of the porousness of our borders, our Canadian border and our border with Mexico as it relates to illegal aliens and the significant number of people that cross our borders illegally without ever being detected?

Director MUELLER. I can go ahead and start on—when the—we in the FBI have in draft form a comprehensive plan for looking at the threats within the United States of various terrorist groups. It is in draft form. It is nearing completion. It does not address the certain areas that I know have been addressed by others, particularly Tom Ridge and his shop, and that is the weakness in the borders. But ours is focused on the threat of terrorism and terrorist groups within the United States. We have to date, particularly since September 11, have done analyses of various portions of the United States where we think the threat is perhaps higher than elsewhere.

But as I said, we have, in final draft form, and it will be completed within the next several weeks, that plan to which the OIG report averts.

Mr. HOEKSTRA. Director Tenet.

Director TENET. Congressman, I think from the perspective of the foreign intelligence community Mike Hayden and I and the components of our community are still very much on our plan, very expanded, that we laid down in 1998. Obviously, we have now expanded the relationship overseas with Mike and our folks and other people, but you've now seen an explosion in operational tempo. You now have seen a far broader reach, and some things I can't say in the open, but in essence the strategy and the targeting that underlay the strategy in 1998 is still now current. Is there a difference. If Afghanistan has changed in a fundamental difference, there are still issues we're working through there.

But when you look at the speed and pace with which we're working together, there is a common understanding of the target. There is a common understanding of the collection and targeting that we engage in every day. It is very fast-paced and iterative, and so that is how we're attacking this problem.

Now, they are intimately involved as well, because they also bring data to the table that allows us to work overseas and also allows them to work here. So there is an integration between the foreign and the law enforcement community against the al-Qa'ida target overseas, and here I might add that I think is quite vibrant.

Mr. HOEKSTRA. The question I have, though, is this morning we spent considerable time talking about holding some folks accountable for not watchlisting individuals so that they would have been caught at the borders or coming in. I got to believe that each of your organizations is concerned that the way that you have described al-Qa'ida and other terrorist organizations is they will gauge us, they will push and they will find our weak spots. And if they find out that, hey, we've got this watchlisting down, you know, we identify somebody. They are on the watchlist. They get to our port of entry. We find them right away. It is not going to take them very long to say let's just get into Canada and Mexico and we'll walk across.

Now, where does that comprehensive plan come into place that says okay, the FBI has got their piece together, the CIA has got their piece, NSA has got their piece, but you guys have your three pieces done, but nobody has taken a look at this border component?

Director TENET. No. Homeland Security and Governor Ridge is looking at the border north and south and it is integrated there, sir. So come to that table and integrate all of that.

Mr. HOEKSTRA. So your plans are being integrated into their plans, and you're providing written documentation, so sometime in the future we can have perhaps a closed hearing where you can present your strategic plans on terrorism in more detail?

Director TENET. Yes, sir.

Mr. HOEKSTRA. Mr. Chairman, I yield back the balance.

Chairman GRAHAM. Thank you, Congressman Hoekstra.

Congressman Peters.

Mr. PETERSON. Thank you, Mr. Chairman. And thank you, gentlemen, for your testimony and for what you and the folks do for the country. We appreciate it.

Director Mueller, I want to talk to you about the Moussaoui situation, and I don't know how much you can talk about this, but there has been kind of ongoing concern in Minnesota about the facts of what happened there that has been an issue. You may or may not be aware of that.

In Ms. Hill's statement for today, the section on page 21 where it talks about that the Minneapolis agent in charge who I think was acting—I don't think there was at that time a—whatever the title is of the person that is in charge of the office.

Director MUELLER. Special agent in charge.

Mr. PETERSON. Yeah. That he was, according to this testimony or statement here, trying to get the people at FBI headquarters spun up, because he was trying to make sure that Moussaoui did not take control of the plane and fly it into the World Trade Center.

And then further on it says that the person at headquarters doesn't remember that conversation.

When we had the gentlemen here that was in Minneapolis, one of the people the other day, I asked some questions about this, and there were some responses that were then later changed. What I'm interested in, if it's possible, is to get on the public record exactly what happened between Minneapolis and the radical fundamentalist unit or the headquarters or whatever it was. Have you looked

into that and are you familiar with what happened between the acting agent in charge in Minneapolis and your folks at——

Director MUELLER. One of the—I am generally familiar with the facts, yes, and not the day-to-day conversations, but I think the breakdown came in that there was a desire to get a court order allowing the agents to look at the laptop and other provisions. There was a disagreement as to whether or not there was sufficient evidence that would link Moussaoui, the individual, to a foreign power which is a terrorist group—doesn't have to be a country, so to speak, recognized country—and there was some disagreements based on a faulty interpretation of the law at the lower levels. That is my understanding. And that——

Mr. PETERSON. Was that in Minneapolis?

Director MUELLER. No. At headquarters. And a discussion with the agent in the Minneapolis office, and it did not get elevated to where it perhaps should have been, either in Minneapolis or —

Mr. PETERSON. I'm not so much concerned about that whole issue because I think we've been through that, but it's my understanding that the agent in charge in Minneapolis actually went above, maybe one or two levels above the place that he originally called to try to get somebody to listen, because they were convinced that there was something going on here, and they were very agitated that they couldn't get anybody in headquarters.

So do you know if the agent in Minneapolis called other people beyond the first person that they called that—where they got into this whole issue about whether they had the—as I understand it, there were calls made to people above that, I don't think at your level, but, you know, people at pretty high levels by this agent to try to get this——

Director MUELLER. I am not aware of that. Hold on just one second.

After 9–11, there were. After 9–11, but not before 9–11 apparently.

Mr. PETERSON. Well, it is my understanding that there were calls made prior to 9–11 to people above, and we keep getting conflicting information.

Director MUELLER. Well, I will have to get back to you on that.

Mr. PETERSON. Would it be possible—and I don't know what the legalities are with the trial and everything. Could you get me the chronology of actually what the contacts were between Minneapolis and who was talked to and——

Director MUELLER. Sure.

Mr. PETERSON. So we can lay this to rest, because there have been some press accounts and concern in the Minneapolis office about what the agent there did and didn't do and whether they did enough and so forth.

Director MUELLER. Well, a couple of things. I would think everybody was concerned about Moussaoui. That is why he was arrested. They were very much concerned about what he might do, which is why the agent made the decision when this came to him to take Moussaoui off the streets on the immigration, and so he was incarcerated during that period of time and was therefore deterred and detained.

I was out in Minneapolis a couple weeks ago and talked to the office and praised them with the agents there and the support and the analysts for the work that they had done in pursuing Moussaoui because I think they did a terrific job. The issue on the disagreements on whether or not you had sufficient information to go forward on a FISA at a particular time did not go as far in the organization as it perhaps should, and we have changed that since September 11.

So if the same situation happened today and there was a disagreement as to whether or not you had sufficient evidence to go forward on a FISA, it would come all the way up to me ultimately if it could not be resolved at a lower level. But I do believe that the agents at the—in Minneapolis did an excellent job, and from day one pursuing it, there were miscommunications back at headquarters that were unfortunate, but it's been resolved.

Mr. PETERSON. Well, if you could get somebody to give me the——

Director MUELLER. I will do that.

Mr. PETERSON. I would appreciate that. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Mr. Peterson.

Congressman Bereuter.

Mr. BEREUTER. Thank you, Mr. Chairman. Gentlemen, thank you for your testimony and for your responses to questions and your public service. In the short time I have available here, I'd like to focus on the future on the basis of the information we know about what has happened.

Director Mueller, I'll start with you just as a follow-up to Congressman Peterson's question, because you made reference to a misinterpretation of the statute by the FBI attorneys related to foreign powers. That was unfortunate. It was probably not crucial, because of the link that otherwise had not been established. But my question to you is whether or not the lawyers and agents across the country now understand the full definition of what is a foreign power so that a FISA determination looks more possible under the two elements in the definition of a foreign power.

Director MUELLER. Yes. We've had training sessions. We also sent out what we call electronic communications to clarify those issues. I will also say the PATRIOT Act is exceptionally helpful in enabling us to utilize that tool in ways we had not done in the past. And we also—there is—there is those of us who have done this work in the past know that when you get a criminal warrant you generally go to an Assistant United States Attorney in the various districta and then go right to the judge there.

So you have the Assistant United States Attorney, the lawyers working with the agents. Part of the problem in the FISA process is there is a FISA court and it sits here in Washington, D.C., and consequently in putting together the package for the FISA court, you have to get the information from the field and meld that information with the knowledge of the court and the procedures of the court back at headquarters and then get the package up to this court. And what we are trying to do is expedite that process by taking out some of the middle people that may not fully understand all of the aspects of the FISA court to make the process go swifter

and to assure that we eliminate, to the extent possible, any room for misinterpretation of what is required under the statute.

Mr. BEREUTER. I think those are very important changes. I'm glad to hear of them.

Director Tenet, do you favor the Homeland Security Department, which we hope will be established, sharing in the tasking of foreign intelligence collections on threats facing the homeland?

Director TENET. Well, I think as a customer, we naturally will take, you know, analytical tasking and whatever help the Homeland Security Department needs we will treat them the way we treat all of our senior customers. So once we get into this back and forth, they will be the recipients of our product in the morning. They will be able to come back to us and say, you know, can you help, would you say this and this? Can you do a piece of work on this? And how it might apply in the homeland, we will naturally do that with them.

Mr. BEREUTER. That is a good accommodation, but it seems to me there are cases where the requirements of the Homeland Security—certainly the priorities on it might be different than they are for the Central Intelligence Agency or the Department of Defense or the FBI, and I would hope that maybe the Senate will do what the House failed to do and give them a seat at the tasking table when it comes to foreign—I emphasize "foreign"—intelligence collection. In fact, I offered that to our Rules Committee to make in order.

I'd like to turn to you, General Hayden, and I recognize what you had to say on pages 9 through 10 of your testimony, which relates to your predecessor, for example, in the '70s and the message we got here from that Congress at that time.

But we've learned that NSA, apparently for policy reasons, decided not to target international communications of individual foreign persons in the USA intentionally, even though it would have been possible, it appears, to obtain approval under FISA for such collections.

Why did the NSA adopt that policy, General?

General HAYDEN. We do get FISAs, but you're right. There are several classes, I'll use the word "targets," in which we would pursue a FISA, and there are others in which we would turn that over to the FBI.

A couple of reasons. One is as you've alluded to before. The history of the agency suggests it needs to exercise great care in what it does within the United States of America. Beyond that, though, no matter who would get the warrant for collection, in this case, NSA or FBI, you would create a seam between two organizations. If we were to get the FISA, the warrant for collection for a protected person inside the United States, we would close the seam between our information gained from SIGINT internally and the information we would get externally through our normal processes.

That seam would be very tight. But the seam would be quite wide between the SIGINT information being gained about that individual and the other information that would be gained by the FBI through all their other tools.

You've got to make a call, and I think in general the call is accept the seam between what I'll call domestically-derived SIGINT

and SIGINT derived from overseas so as to put all the general you're getting about this person inside the United States into one basket under an FBI rubric so that all the tools being used to gain information about this target——

Mr. BEREUTER. Including your assets?

General HAYDEN. And then when asked by the FBI—and this is commonplace—the FBI would ask us for technical support, but the action would be carried out under their authorities.

Mr. BEREUTER. Thank you. My time is expired, Mr. Chairman. Thank you very much, gentlemen.

Chairman GRAHAM. Thank you, Congressman Bereuter.

Congressman Roemer.

Mr. ROEMER. Thank you, Mr. Chairman. I just want to say that I really respect the difficult job that the three of you have in front of you. We have, in our past 50 or 60 years ago, had an enemy that was trying to take over all of Europe, and we knew how to go after that enemy. We had an enemy in Vietnam that used guerrilla tactics, and we had difficulties there, and now we have an enemy that tries to train on our own soil, tries to infiltrate our own schools and tries to kill hundreds, if not thousands, of Americans. And we count on you three to help protect the security of this country.

Now, while there are people, maybe, on this committee that think that the three of you may be to blame for many things, lots of things, everything, and there may be some people on this committee that think that you performed flawlessly before 9–11, I come down on the side of I believe mistakes were made. I believe there were failures. I believe that there were inadequate communications between agencies.

So we didn't have enough linguists and analysts, that we didn't have a good enough watchlist system, that we could have had newer technologies in different parts of our country in our field offices. But I am for moving forward and try to make sure in light of what happened in Kuwait, what happened in Yemen, what happened in Bali, what happened in the Philippines today, killing six people, injuring 144 people, that it doesn't happen in this country again, and that we move forward and try to correct those mistakes, and I think the three of you are the three people to help lead us there and get us there. I have confidence in the three of you.

I also think that this joint inquiry has done a magnificent job, Mr. Chairman. I'm proud to serve on it with the ranking members, and we have to work to uncover facts, to try to make recommendations to solve some of the problems and fix some of the mistakes while not just saying this is a witch hunt and a blame game.

Now we have, in a bipartisan way, come forward and said we need a joint commission. You folks are busy. You don't have a lot of time to look back, but we do need to correct the mistakes. We're about ready to go out of business with this Congress ending. We've got thousands of pages of documents that we still have to go through. We have some major institutional recommendations that we might need. We need an independent commission to finish the work, and we have agreed to do that.

And the House and the Senate in conference and the White House keeps moving the goal posts on us. We've solved one problem, and they change the goal post and say, well, here is another

one. I would hope the White House would come forward and work with us. They've negotiated with us. But genuinely work with us to create this independent commission and help us, help you three, help the very good people that work for you that dedicate their service and their lives to protecting Americans to getting this right in the future.

I have just three basic questions, one for each one of you.

General Hayden, you said in your testimony that you don't need to be reminded about linguists. I think you do, all due respect. In your 2002 fiscal year request, you asked for significantly less civilian analysts and linguists. I know you are a level three expert. You speak Bulgarian. We vitally need these linguists doing their jobs and these analysts doing their jobs, strategic analysts and tactical analysts. I'd like to know why, just in the latest '02 budget you haven't requested more than the previous year. Let me get all three questions in.

I've learned that on this committee, that you've got to get your questions in.

Director Tenet, I just ask you very quickly about sharing information. You mentioned in your testimony that you are acquiring some very significant information for us in Afghanistan in safe houses and other places. We hear some grumbling that that information is not being shared with other intelligence agencies, not only quickly enough but at all, and I'd like to get your thoughts. In fairness, is that a legitimate complaint? How are you sharing that?

And lastly, Director Mueller, I would ask you, do we have in place now, a year and a month after September 11, the necessary computer networks to compile counterterrorist information in common, common databases between our district offices and the FBI across the country and with headquarters, and how do you disseminate that information?

General Hayden.

General HAYDEN. I'll go first, yes, sir.

The reason we don't need to be reminded is I think we get it. We agree with you totally. We hired 120 in fiscal year '02. We've hired 11 so far in the first 16 days of fiscal year '03. We've got another 101 in the pipeline for—to whom we've already offered conditional employment. So we've got it. We're working hard on it, and I take your point.

Director TENET. We've just sent a piece of paper to the committee, Mr. Roemer, about this so-called Docs X issue, where I've basically written a document that NSA, DIA, the whole community signed up to basically have a common repository. We will build a national center that we fund to basically train the right people, and we have put in place procedures that make it clear what is in and what is out with the expectation that whatever limited information is kept out for real operational reasons will be stripped and moved as fast as possible. I know Mr. Burr has been briefed and we'd be happy to come brief you as well.

Mr. ROEMER. Thank you.

Director MUELLER. As to the question of whether the FBI has the technology in police stations now to share all common databases

around the country, the answer is no. I will tell you what we have done, however.

We have and are redoing our technology. One of the key aspects of that is to migrate the data from what we call ACS into a new Oracle database and put on it a user interface that completely changes the way we have done things in the past. And the target date for that is December of '03.

In the meantime, however, because of the necessity to pull together data relating to terrorism, we have holed in at least three data streams into a database. One of those streams are all of those approximately 23 million pages of images that relate to terrorism throughout the FBI. On the second part, the second data stream will be any of our electronic documents from ACS from 1993, on that relate to terrorism, will go into that database.

And the third stream is the cable traffic from the Intelligence Community that—both internal and from the Intelligence Community, and actually the fourth data stream is the information that we picked up from Afghanistan.

All of those data streams will be in a common database within the next 30 to 40 days. That database will have the capability—we will have with that database structure the capability utilizing the search tools that we have not had the capability to use before.

The other aspect of that is we have not had a capability, we have not had a LAN, a local area network within the Bureau that is at the top secret SCI level. We have put in that—are in the process of putting in that LAN so that our analysts are, can have that—access to that database on the one hand and have new information that comes in pushed to them according to certain profiles in a way that occurs in the CIA. So even though across the FBI we will not be where we would want to be in the next 30 or 40 or 50 days within the counterterrorism sphere, we have made strides.

Mr. ROEMER. Thank you for the extra time, Mr. Chairman.

Chairman GRAHAM. Thank you, Congressman Roemer.

Congressman Reyes.

Mr. REYES. Thank you, Mr. Chairman, and gentlemen, I would like to associate myself with the comments of many of our colleagues here that are appreciative of your service and the leadership that you show, and I also agree with Congressman Roemer that you are the exact three individuals that are going to be very instrumental in helping us address this challenge.

I'd like to start out by telling all of you, in particular, Director Tenet and my colleagues that referred to the homeland defense legislation that is pending, I wanted to reference also General Hayden's comments about not having to be reminded about Arabic linguists and that we have a role to play in terms of determining where the lines of privacy rights versus government's need to protect the homeland are.

And you referenced Director Tenet's comment that we need to get it right. And I absolutely agree with that. And, Mr. Chairman, I voted for homeland defense, but I will not support homeland defense if the national police force amendment is in there. I will not support homeland defense if we don't have the protections of civil service and labor in there as well.

And I won't support it because of a concern that I've expressed to you, gentlemen, and that is diversity. I go back 33 years ago when I first came back from Vietnam after serving my country, was hired by the Border Patrol. There were only three of us that were Hispanics in that class, and had we not had the protections of civil service and labor rights, I would not have had a 26½-year career in the U.S. Border Patrol.

And I just wrote a letter to the President this week, telling him that the flexibility that he seeks is one that I think will doom minorities in the 21st century from participating in homeland defense, in the FBI, in the Border Patrol and in all the Federal agencies, and I say that because of my experience. So I support the homeland defense agency, but, again, will not support it if we don't have those kinds of protections.

I was intrigued by a comment that you made, Director Tenet, in terms of the alerts and the information that is out there and the fact that we have to sensitize our country to understand that the threat is real. We've had testimony here that has told us that the safest place for a terrorist is in this country, because of all the protections that we have and your reference, General, to bin Ladin crossing the border and then all of a sudden getting the protections.

But I strongly believe that that's what has kept us as the best experiment in democracy that we're being attacked for. So it reminds me a lot, Director Tenet, of the alerts for 13 months I was in Vietnam. It became a joke that if we were told that we were on red alert, that our base was going to be hit, that you could bet we weren't going to get hit or rocketed that night. But if we weren't on alert, we'd get hit. So my question to each of you—and I don't know, General; I also want to include you in here—is regarding threat assessment.

I know that, Director Mueller, last week the committee received a copy of the Justice Department IG's report, where it noted that the FBI has never performed a comprehensive written assessment of the risk that terrorists present to this country, and I'm wondering are you engaged in that now, and also Director Tenet, what is your role in that process? And also General Hayden, if you would—I know that five minutes is not long enough to cover all the things, but, you know, I want to make sure that we're not going to get in a situation where we treat the symptoms and we don't treat the disease. And so if you would address the——

Director TENET. Sir, we're preparing just such an estimate that the FBI and NSA will be playing into in the process in the next few weeks. So we will have that kind of comprehensive judgment. We will take Bob's information and obviously the other intelligence information and have it in a package, and obviously, given the importance, we'll update it regularly.

Mr. REYES. Will that include recommendations of how to fight the threat? Because, you know, as someone in Congress, after spending 26½ years in Federal law enforcement protecting the border, I don't want our country to have to deal with martial law. Everybody is worried about the sniper in this region right now, and they are talking about bringing in the military assets and all of these other things, but I think terrorists win when we subject our-

selves to martial law and those kinds of issues that I mentioned before in my opening comments. So will that include——

Director TENET. Sir, we won't typically put policy solutions in the estimate, but I'm sure we can then use it as a vehicle with Homeland Security Council and sit down and walk through it and see what additional measures that may be required as a result of what we can tell.

Director MUELLER. Let me just—one thing you mentioned about the use of military resources, and you mentioned it with regard to our current investigation into the sniper. And let me just say that the resources are limited to support in terms of giving us the capability that we did not have, but law enforcement remains law enforcement, and the military is not playing a role in the law enforcement function on the ground.

General HAYDEN. I'll just repeat what I said in my prepared statement. One of the charges I gave to our workforce is we're going to keep America free by making Americans feel safe again. I know there will be unbearable pressures to limit our civil liberties if we have repeated events of 11 September.

Mr. REYES. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Congressman Reyes.

Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. Let me begin, if I might, with you, Director Tenet. I have been digging into the process for how intelligence documents become classified, and I'm increasingly concerned that the CIA and other agencies are designating too many documents as classified and, in effect, out of reach of the public.

Now, my concern has really been heightened by the fact that after 9/11, the President of the United States, and correctly, in my view, has been urging the public to help win the war on terrorism, to get involved and contribute and assist in any way, but that is going to be pretty hard to do when key information is kept from the public that would let them, in effect, pick up on the suggestion the President makes.

And what I'd like to do is get your sense. Particularly with respect to threat analysis and threat analysis, my understanding is generally classified as secret or even higher.

Now, with threat analysis there is a substantial amount of analysis that, in effect, reviews terrorist tactics and procedures in a pretty general sort of way. Information could help the public, for example, know what the terrorists have done in the past, what they may be considering in the future, but it isn't going to compromise a sensitive, ongoing operation by providing excessive detail about a specific threat. So my sense is that if we got away from this process of overclassification and provided this information to the public we could do more of what the President of the United States is suggesting and act in the public interest.

So my question to you is, why can't more of the terrorist threat analysis, the kind of information I'm talking about, be declassified and shared with the public?

Director TENET. Well, sir, I think you missed my statement earlier and my long statement. I said a couple things. One, it's very clear we have to move information to a whole different set of cus-

tomers in the context they need to receive it in. I'm talking about police chiefs, other people who fall outside of the Intelligence Community. And the important thing is that we have to find ways, write things that are content rich that compromise many of those things and we ought to be able to do it. Because otherwise I think we can isolate all this information. And today, you know, when Governor Ridge or anybody speaks, we do that for them, but it is very clear that the information we possess, or that the FBI possesses, has to go out certainly to the lowest denominator in the country working the problem—police chiefs, governors, mayors, others, the public—and we're committed to trying to do that. You know, when the fate of the country is at stake, we have to do a better job of moving to that customer base the way we take care of the military or the State Department or others. We have to figure out how to do that.

Senator WYDEN. Will more terrorist threat analysis be declassified? I continually hear about how we're going to make changes and we're going to look down the road at this and that, but I don't see anything actually happening. I'm asking you about a specific area that I think could be declassified in a very specific way. So if you would respond to that, can we expect to see a change in classification policy with respect to terrorist threat analysis?

Director TENET. Sir, we will do our best. Yes, we're working with Homeland Security, and I'm committed to trying to do this.

Senator WYDEN. Well, I will follow up, because we've only got five minutes, but I want it clear today to you and also to Director Mueller. This is going to be a central focus of my work on this committee. I think that too much is being classified now. It runs directly contrary to what the President is wisely counseling. I think it has got to change.

The only other point I wanted to make, and I know time is short, is Director Tenet, as you know, I and others have been working on putting a terrorist identification classification system into the intelligence authorization with Senator Shelby's support and Chairman Graham's support. I think we're going to be able to do it. It would stand in sharp contrast to the State Department's TIPOFF system, which really only gives limited information to a limited number of Federal customers, and really doesn't even get to the State and local people.

Tell me, if you would, in the time I have how you would meet the requirements of this legislation and get the necessary information out, not just throughout the Federal Government, but to the State and local people as well.

Director TENET. I'd like to see the legislation, and I'll work with you and figure out how we do that, sir. I don't have an answer off the top of my head, maybe I'll sit down and talk with you and figure out how we work this together.

Senator WYDEN. Well, we'd like to do that, and we have supplied it to you. And we'll do it again. Thank you, Mr. Chairman.

Director MUELLER. Mr. Chairman, can I just have a second to respond to Senator Wyden's concern about getting information out to State and locals and the legitimate concern about how we can strip out this information from sources and methods and push it out?

We had started, in the wake of September 11, a weekly bulletin that goes out every Wednesday to every one of the police departments in the United States that provides that type of information. It probably needs to be expanded on, but it does provide the information that the police officers need on the beat as to what tactics, what they should look for in terms of what terrorists are doing, and I'd be happy to provide you the series of bulletins that we put out over the last several months.

Chairman GRAHAM. Thank you, Senator Wyden.

We've now completed the first round of questions. Starting the second round, we'll try to wrap this up in the next 30 minutes or so.

I'm going to ask questions which follow up on my first round of questions, which had to do with how we're going to respond to this probability of Saddam Hussein reacting to our attacks against him. But I'd like to make a couple comments building on statements that our members have made.

The first is to Director Mueller. It is my understanding that the issue that both Congresswoman Hoekstra and Congressman Reyes raised relative to the comprehensive study of the terrorists who are embedded in the United States was initially requested in 1999. If that's correct, is that a correct statement?

Director MUELLER. I'm not certain, but I have not looked at the testimony. I know that we have had it in process, and it is in draft—final draft form.

Chairman GRAHAM. I think that is critically important, because if our people start to see as the CIA intelligence estimate speculates or states is a probability, which I understand in CIA terms means a 75 percent or better chance of becoming reality, if they start seeing these increasing waves of attacks here within the United States, there is going to be hell to pay. And I think we need to do everything that we can in the time that is available to us to try to build the strongest protection.

My second comment goes back to my initial question, and that is that this program of trying to deter the international terrorist has both the defensive component here at home and the offensive component abroad. I think we've done quite a good job of dismantling the capability of al-Qa'ida, although we now seem to be in a stage of some regeneration.

My questions have to do with what are we doing now, particularly in terms of preparing through enhanced intelligence assessments, to begin to dismantle the other terrorist groups who might be the linkage for Saddam Hussein to attack us here at home, groups such as Hizbollah that have been mentioned in your earlier testimony.

Director Tenet, you have made a very appropriate comment about sanctuaries being a key part of this. We know what an important role they play for al-Qa'ida in Afghanistan. Today a substantial number of the sanctuaries are not in Central Asia but in the Middle East in places like Syria, the Syrian-controlled areas of Lebanon and Iran. Yet in a meeting that Senator DeWine and I had with the President of Syria, he denied that there were these training camps under his control.

One of the things I would suggest is we ought to do to Syria what apparently we did to North Korea within the last few days, and that is lay down the evidence we have, which I think is quite compelling, and confront them with it, and maybe it will cause those governments which are currently housing those sanctuaries to take a greater sense of responsibility in dealing with them. And if they don't, I think they should know that we're prepared to do so. I wonder if you could comment on that string of suggestions.

Director TENET. I understand the argument about the sanctuary. Obviously I've made it with regard to al-Qa'ida. I think you really—you're asking a bunch of policy questions. It's safe to assume we're working against all those groups without going into it here, but I think you have to also—we're in a big war right now. I think the sequencing and thinking and obviously when we talk about terrorism, we're not limiting it to Sunni extremism. We're not limiting it to just one set of groups.

I think the point you make about you ultimately have to put more pressure on people to rid themselves of people who, whether they allege they command and control or don't, still use their territory as safe havens. And all you have to do is talk to our friends, the Israelis, to understand the implications. These groups are continuing to operate there.

Chairman GRAHAM. Are you satisfied today with our efforts, and specifically what you've been tasked to do to put us into a position to begin to dismantle these terrorist groups abroad and deny them the sanctuaries?

Director TENET. Sir, I'd like to talk about that with you in closed session.

Chairman GRAHAM. Okay.

Senator Shelby.

Vice Chairman SHELBY. Thank you, Mr. Chairman. Just picking up on your word here, it's one thing, Director Tenet, to perhaps dismantle them, and I think you have. We have, and they have, all of you, in some ways, but at the same time by dismantling them, you've dispersed them.

Director TENET. That is an opportunity, sir.

Vice Chairman SHELBY. Opportunity?

Director TENET. That is an opportunity. When you get people moving, that is opportunism.

Vice Chairman SHELBY. Because they are on the run, aren't they?

Director TENET. Yes, sir. That creates plenty of chaos in the system.

Vice Chairman SHELBY. I want to get into something else. I want to pick up a little bit on what Senator Levin was talking about earlier, and this afternoon late here, I'm not here to get into a semantic debate on the meaning of the word or term "accountability." Obviously the word "accountability" means different things to different people. To some people it has no meaning, literally no meaning. To others where you have real feelings of responsibility, it equals—accountability means, perhaps, responsibility, you know, in that context.

And it is troubling to me, and it was to Senator Levin and to others on this committee, that it seems from your testimony and other

evidence that the staff has collected that no one is responsible, you know, in the CIA.

Director TENET. No one is responsible for what?

Vice Chairman SHELBY. For the failures. In other words, no one is accountable. No one is responsible. No one is responsible at the Bureau, at the FBI. No one is responsible. In other words, it is no one's responsibility. That is troubling, very troubling. To each of you, what does the term "accountability" mean to you? I'll start with General Hayden. In this context, you know, if you have a job to do, and if you do it in a slipshod way, and there's no measure of performance, or if it is, nothing happens, go ahead, General.

What does "accountability" mean to you, sir?

General HAYDEN. There is a difference between a job not being done and a job being done in a slipshod way.

Vice Chairman SHELBY. That's right.

General HAYDEN. And I think what Director Tenet was pointing out, the issues that this committee and our dialogue have uncovered are systemic issues, that we put people in situations in which they had inadequate tools or inadequate circumstances to succeed.

Vice Chairman SHELBY. But not always. General, we'll all concede that you need more resources, and we've worked with you, Senator Graham and other members of the committee, to revamp as a priority NSA and you're working toward that goal. We have to. We've worked with Director Tenet.

Director TENET. Yes, you have.

Vice Chairman SHELBY. I'm not on the Judiciary Committee or the criminal justice appropriations, but I know others have worked in that regard. I know you don't have too many resources, but a lot of this is decisions that people make or fail to make.

Director Tenet.

Director TENET. Well, sir, let me just say——

Vice Chairman SHELBY. What does the responsibility, accountable mean to you?

Director TENET. Sir, when you look at this, I look at it in the following ways. Look at anybody's performance and say, tell me about the integrity of the individual, how hard they were working. Tell me about their understanding of their job. Tell me about whether they were slipshod. They will me about whether they were paying attention to detail and doing everything they knew how to do.

Now, when somebody——

Vice Chairman SHELBY. Let me stop you a minute. Let me just say, knowing everything they knew how to do, but what if you had people in these jobs that didn't know what they were doing and didn't know the standard? And I know some people at the Bureau—we had testimony here—didn't know the FISA standard, even lawyers over there, Director Mueller. I'm not saying it's your fault. I'm just saying that they are inadequately trained.

Go ahead, Director Tenet. I'll try not to stop you again.

Director TENET. No, sir. It's okay. Keep going. I lost my train of thought. I apologize.

Vice Chairman SHELBY. Maybe you'll pick it up again.

Director TENET. I was on a roll.

Vice Chairman SHELBY. You thought you were. You weren't on a roll.

Director TENET. No. I was on a roll, sir.

Vice Chairman SHELBY. I don't think so.

Director Mueller, what is your feeling—or how do you feel about the word "accountability," the term "accountability"? Is that responsibility in that context? What does it mean?

Director MUELLER. I think it is giving people both the responsibility and the authority to do a job, to set out parameters, what you expect from people, and if they do not live up to those parameters, then you hold them, quote, "accountable."

Vice Chairman SHELBY. Hold them or——

Director MUELLER. Yes. Absolutely, but the ultimate accountability is me, and I have to set those standards. I have to give them the tools to do the job. It does not make any sense for me to hold somebody accountable if I have not given them the responsibility, the authority and the tools to do the job. That is just—that's wrong, and so in terms of something like the training on the FISA issue, it's the responsibility of me to assure when I see something like that, that we put into place the mechanisms to get those individuals trained. If we did not give them the training, I cannot hold accountable that person who was inadequately trained, because I did not provide the person with that training.

Vice Chairman SHELBY. I want to pick up lastly on Senator Levin's statement, paraphrase him. Has anyone in the CIA or the FBI been held accountable for the failures thus far of September 11 or the events leading up to it? Director Tenet.

Director TENET. No. And there is a reason. We're in the middle of a war.

Vice Chairman SHELBY. Oh.

Director TENET. We're in the middle of a war, sir.

Vice Chairman SHELBY. That is not an excuse. Director Tenet, Let me tell you something.

Director TENET. It is my judgment to make, tell.

Vice Chairman SHELBY. No. It is your opinion. Let me tell you what happened. Do you know in the Second World War when we were in the war, that there were just dozens and dozens of generals that were—and captains of ships, especially the submarines, that were—that were replaced immediately. You ever heard of Kasserine Pass, Anzio Beach and such things? They jerked generals out of the war and put people in.

Patton went into Kasserine Pass after Rommel defeated the American forces in Anzio Beach. I forget the general's name, but he was supposed to have been, you know, the up-and-coming general. He was brought back stateside. I think there has to be accountability. That is what Senator Levin was talking about. I think you ought to go back and look at the work—the real meaning of the word.

Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Senator Shelby.

Congresswoman Pelosi.

Ms. PELOSI. Thank you very much, Mr. Chairman. Gentlemen. I want to also commend the members of our committee for their very wise judgments that they are bringing to this joint inquiry, and wisdom is what we need now because certainly we have to have accountability internally within the agencies and externally up the

chart to the President of the United States. We also don't want to find a scapegoat and say we've solved it—but for that we would have not had September 11.

We really have to protect the American people in the future. So we have to be, I think, judicious in how we evaluate any one piece of information and how it all relates to one another and what the accountability is.

I have serious concerns that part of our civil liberties may be part of the price we pay for our falling short in areas where we should have done better. So I think after we go through all of this, we step back and try to make some evaluations without declaring something the cause which would be a false sense of security to the American people.

I have a couple observations. First of all, I don't want the day to go by, Mr. Director, without saying to you, Mr. Tenet, that I've looked at the legal—what we want is to find the truth, and that is why many of us have advocated things that we've talked about earlier in terms of the Commission, et cetera, and we want more openness wherever possible, and certainly we don't want to jeopardize sources and methods or legal cases or whatever, but we want the truth, and we want openness.

And I looked at the legal justification for keeping classified the government positions to which certain intelligence information was provided, and I think the legal arguments that were made were not compelling, in my view, and I think it is a misapplication of the classification standard.

Moving on from that, again, back to my main point about opportunities that were there which may or may not be dispositive of this issue as to whether we should have known, could have prevented and are helpful in the future, but there are certain windows—the Moussaoui window, windows of people coming into San Diego. I happen to think—we're trained in this committee, as all of us are, I think, that force protection is our first priority to protect our young men and women in uniform wherever they are, not only when they are in battle, but also wherever they are, and I would hope that in the future, we would see the vulnerability we have when somebody comes into San Diego, for example, which is rich with servicepeople and installations, that we would be even more careful, even more careful, because of the exposure we would have to our forces there, recognizing, of course, we want to protect all of the American people.

It's interesting to me, Director Tenet, that you—did I conclude correctly that the arrest and apprehension of Moussaoui may have hastened these folks to move on more quickly?

Director TENET. It is just a judgment, Ms. Pelosi. And I could be wrong. It is a personal judgment.

Ms. PELOSI. I appreciate your reinforcing that judgment.

In your testimony, it contains many instances, Mr. Tenet, in which strategic warning was priored about the possibility of terrorist events or attacks. Your testimony contains few, if any, instances in which tactical warnings were provided about a specific attack to occur at a specific place, specific time. Tactical warning, of course, is by definition actionable. Strategic warning suggests general action, if any. Strategic warning tells us something bad

may happen somewhere at some time. What action should flow from this type of warning? What is the value of that type of warning that we can—how can we act upon that?

Director TENET. Well, Ms. Pelosi, what we tried to do when you read through the testimony and look at the disruptions and all the things, we tried to change the balance. And when we couldn't get a tactical warning, we tried to get things moving so we could generate more information to stop things. There was a stream of things that were stopped here. No numerous places and attacks and individuals that we apprehended who were going to—so what you're trying to do through this kind of planning is make your luck, be disruptive enough to collect additional information, have operations, drive analysis to give you the ability to figure out if you could ever get that tactical warning. And that's the hard part of this business.

Now, I'd say, you know, if you look at where we were last year compared to this year, we're much better in that regard overseas. The disruptions and information we've collected have not only given us tactical warning of events that were going to occur overseas, it has given us real and valuable strategic insights into targeting and planning that we can then provide, perhaps, to homeland security or other means. So it's a dilemma. It's always that when is the date, time and place of an event.

Ms. PELOSI. Or even something narrower than—we always say in California that people have predicted ten of the last two earthquakes. They are always saying there is going to be an earthquake. And then a couple of times it happens, but that is pretty good, two and ten. That is pretty good. At least then we have some idea where these things may happen because of the fault lines.

We have to have a better idea of the fault lines in the U.S. so that our strategic warnings can be narrowed down to more tactical warnings. It appears that my time is up. But if anybody would like to make any observation on that, I am sure the Chairman and his generous gavel would allow.

General HAYDEN. Ma'am, I understand exactly what you need. Frankly, we did very well in the summer of 2001 with strategic warnings. It was the tactical warning that was missing. But the analog to the fault lines is one step short of a perfect analogy. And simply this, our fault lines change their minds. They decide not to crack because of our issuing warnings about the fault lines. So it is a more difficult thing for us to measure.

Ms. PELOSI. I appreciate that, General. We do have areas of exposure. As a mom, as a person who protects her children, her grandchildren, my husband and I, you know where your exposure is. So you have to make sure that those windows are closed and locked and whatever else that you do to protect your family is taken care of.

And I think that we had exposure, internationally even. We had exposure with the *Cole*, we had exposure in East African embassies, we had exposure in Khobar Towers, and internally we had exposures at our airports, which brought such tragedy and sadness to the American people and to the families.

Thank you, General, thank you, gentlemen. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Congresswoman Pelosi. Congresswoman Harman.

Ms. HARMAN. Thank you, Mr. Chairman. I just want to mention that from here I can barely see, but can I see the pictures of some who perished on September 11. I appreciate that, that you bring those pictures into these hearings, because it keeps us focused on something very central to what we are looking at.

I want to change the subject to something mentioned in General Hayden's testimony, I think only in General Hayden's testimony; that is technology. He was clear about the fact that about a third of his technology is in-house and that will go down to about 18 percent shortly. And he was describing some of the new contracts he has let with the private sector.

I represent the district that probably makes more of our intelligence architecture than any other district in the country, and if it doesn't now, it certainly will under my leadership. But, nonetheless, I think it does now.

And I think that that is wonderful. I commend the people who make it. I think that the cutting edge technologies reside outside of the capacity of your departments. You obviously know that at NSA, the CIA knows that, that is why you have set up IN–Q–TEL, which is a venture capital firm that procures emerging technologies for you.

I think that has been a very successful venture. And I commend you for doing that. Again, a lot of Californians are on that board; it is a good board. To you, Director Mueller, I think when one thinks about technology you are the one who has to play the most catch-up. I think most people think—that that is not a food, the way I pronounced it. Most people think that the FBI was in the dark ages or maybe pre-dark ages before 9/11.

The notion that you didn't have e-mail systems or I don't think that you did, or you didn't have interoperable anything, is pretty horrifying. And I know, Director Mueller, that you are moving fast to correct all of that. But my question in my two remaining minutes to all of you is, how do you assess the importance of technology, and not just for your individual agencies but the importance of figuring out the digital systems that we will need to connect us together, connect the humans together, connect the information dots together, and do the kinds of data mining and other things that will augment what the overworked human forces that you have there can possibly produce, even under the best guidance?

General HAYDEN. Ma'am, it is the war winner for us. I don't mean just because it happens to solve this particular problem, which it does. It is an expression of the strength of the American people. As an airman, I am fond of saying the American Air Force is the military expression of the American aviation industry.

With regard to NSA, we are the security expression of the American computer and telecommunications industry. We as a Nation need to play to our strengths. That is our strength.

Director TENET. I can't add anything better than that.

Director MUELLER. We have to—adopting technology in the FBI, going from a paper-driven organization to a digital organization will free us up, make us more horizontal, remove a lot of the bureaucracy that we have heard about in the course of these hear-

ings, give us new opportunities, give new opportunities, investigative tools. But I will add one caution, that with that new technology has to come training, has to come user friendliness, has to be changes in job descriptions, has to be changes in procedures.

It is one thing to bring in boxes. You can bring in computers, you can bring in the software, you bring the hardware. But if you did not provide the changed business practices, if you did not provide the training, if you did not provide the user friendly interfaces, then you will be going no place.

And so while people talk of technology, you can't talk of technology divorced from what you are doing throughout the organization. And to the extent that we can adopt the technology and change the organization, it will give us the freedom to be far more agile, flexible than we have been in the past.

Ms. HARMAN. Well, I agree with that. My light is on, but I would just add that we are confronting a digital foe. Those who threaten us know how to use technology. They don't necessarily own it, but they imbed messages in other communications architectures, and we are discovering that finally. It is a good thing that we are.

But, we need to be one step ahead of those folks. One of the additional features of the Homeland Security Department legislation we keep talking about is a front door for emerging private sector technologies that should help us get one step ahead of the terrorists.

Director MUELLER. Can I make one response to that? If I could, Mr. Chairman. That is, while I say we are behind in providing our agents the technology that they need to centralize, analyze and disseminate the information, we are on the cutting edge, I believe, when it comes to investigating any aspect of computer crimes, whether it be denial of service attacks or worms or viruses or hacking attacks and the like. We have to build on that expertise that we have in-house as we develop the technology throughout the organization.

Ms. HARMAN. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Congresswoman Harman.

As Senator Shelby has already done, I am going to have to leave at this time. I wish to again express my appreciation for the service that each of you gentlemen is rendering to our country and for your service to our joint inquiry today.

I am going to turn the gavel over, as directed by Co-chairman Goss, to Congressman Bereuter, who also will be the next questioner. After we complete this, the last of our public hearings, our task will turn to preparing a final report with recommendations.

We had three assignments. One was to attempt to determine what happened on September 11; second, why it happened; and, third, and I believe most important, what should we do about it? To that end, the committees will meet again, possibly during the adjournment of the Congress, in accordance with the rules that govern the convening of the meeting of the two committees, to commence the process of completing our task by completing our report and final recommendations.

As this might be the last public opportunity to do so, again I want to express my deepest appreciation to Ms. Eleanor Hill and to her outstanding colleagues who have placed us, I think, in such

an advanced position to have told the American people with a clarity and cohesion that I do not believe that they probably had, what did happen and why, and now accept the challenge of answering the question what are we going to do about it.

With those challenges still ahead of us, I say thank you.

Mr. BEREUTER [presiding]. Thank you very much, Chairman Graham. We just have a few Members yet, it appears, to complete the questioning of the second round and the hearing.

I will begin my comments by saying that I think we should try to learn what we can from foreign counterparts, to the extent that it might be relevant and consistent with our own values and governmental system. Accordingly, I have a couple of questions in that vein. And, Director Mueller, I would like to direct the first one to you.

Scotland Yard has a system of special branches that pass sanitized intelligence information to the police and to the private sector. The British Security Service sends staff to the special branch offices. This gives them a national reach. Do you believe this approach could work in the United States? Why and why not?

Director MUELLER. Well, I think aspects of it certainly could work. I think our joint terrorism task forces that we have set up around the country are a variation of that type of system. We are far larger than Great Britain. We have something like 18,000 police departments, 17,000, 18,000 police departments throughout the United States. And we are unlike Australia, Canada, which has the RCMP or Great Britain, and that distinction makes a big difference. We are a democracy, and we are democratized in our policing within the United States.

And the joint terrorism task forces, in my mind, are mechanisms whereby we can accomplish the same kind of sharing that is done by Scotland Yard. One of the things that we are doing is that we are integrating in the task forces individuals from the CIA in the countries so that we have ready, on scene, that type of information from—that is inside the CIA computers that can match up with the information we may have in the State and local level, which, in my mind, goes some distance towards accomplishing what the MI–5 model does in Great Britain.

I think we have got to do a better job of that.

Mr. BEREUTER. Thank you, Director Mueller. You are certainly right to point out the differences in our system and especially the size of our country and the number of police departments. But I have noticed that the information technology which you were just getting into in the end of your comments that is being employed now, putting in—being put in place in the United Kingdom, seems to have filled some of these needs, even for a vast country like our own with different political subdivisions and different responsibilities. I notice that it is being done largely with American consulting and IT firms.

Director MUELLER. It has always been my cherished hope that we could, throughout the United States, standardize computer input for police departments. We tried to do it on the East Bay. It is being done in St. Louis and the like, because from county to county, police department to police department, we have no standard for the input of things like names, dates, and the like. Stand-

ardized fields, standardized records. Were we to have that in the United States, we would have the foundation upon which to exchange the information that we want to exchange among the various law enforcement entities. But we are a far ways from doing that.

Mr. BEREUTER. Thank you. General Hayden, the Attorney General, as you may be aware, recently approved new guidelines to govern the conduct of counterterrorism investigations under the new USA PATRIOT Act and the FISA statute.

I understand the Department of Justice has established a training program for that, and the CIA is a participant in it, a full participant, as I understand, so that this kind of information-sharing about the proper use of these tools will be available.

Are you aware of the training and, furthermore, most importantly, is NSA going to participate in it?

General HAYDEN. Absolutely, sir. Let me tell you, for our narrow purposes what the PATRIOT Act has allowed us to do is to more readily, more quickly, more completely be able to share information of foreign intelligence value derived from FBI FISAs. That has been a major step forward for us.

Mr. BEREUTER. Thank you. Director Tenet and/or Director Mueller, to both of you, the MI–5—again back to the United Kingdom—and its sister foreign service, the Secret Intelligence Service, work on international terrorism jointly. They determine which service is best placed to handle a target and pursue targets collaborative.

Because international terrorism respects no borders, the service responsibilities in this area are blurred. This eliminates the need for hand-off from one service to another, which has been, at times, a problem in our own country. What are your views on how this could be implemented in the United States?

Director TENET. We do it today, sir, in terms of working overseas with his Legats, and working with our chiefs of station. We started this four or five years ago. We do this today.

Mr. BEREUTER. Do you feel there is any difference in their ability to avoid a hand-off problem because of their arrangement that you cannot or are not now matching?

Director TENET. No, sir. I don't know the precision of what their arrangement is. I will take a look at it. But I know that our arrangement in terms of how we exchange information and make determinations of where primacy lies and how we hand off to each other has been working quite well for a number of years overseas. We are very pleased with where we are.

Mr. BEREUTER. Director Mueller, do you have any comment?

Director MUELLER. I would agree with that. I think it—we need to do it better. We ought to have enhanced exchanges. I think with the FBI's transformation of its technology capabilities that it will much enhance our ability to be integrated, integrate our analysis, integrate our systems.

But I think we have done—come tremendous ways, particularly in the last four or five years, especially since 9/11. We are doing things we didn't do prior to 9/11. I think the hand-off is very good now, certainly far better than it was prior to 9/11.

Mr. BEREUTER. And the hand-off problems that we focused on are primarily on homeland security issues during the course of this investigation.

My time has expired. So I am pleased to yield now to the gentleman from Indiana, Mr. Roemer, for five minutes.

Mr. ROEMER. Thank you, Mr. Chairman. Again, we very much appreciate your time. You have been here for 6½ hours and skipped your lunch. We hope you don't skip your dinner as well.

I want to be brief in asking a couple of questions about progress in the war on terrorism, and maybe you can be brief back with me too.

My constituents often ask me, how do we gauge the success in this war? It is tough to quantify, it is tough to explain. Director Mueller, how would you explain it to them in regards of what progress have we made on the anthrax investigation? Can you update us on that?

Director MUELLER. Well, there are several aspects to the investigation. One is looking at particular individuals. We still have individuals that we are looking at there.

Another aspect of the investigation is identifying the chemical composition of the anthrax that was found in the Daschle and the Leahy letters and comparing that anthrax to the anthrax that was found in the letters that were mailed to The Post in New York, and to Brokaw. And the chemical and the DNA analysis of those samples is ongoing.

We are utilizing that process to compare those samples to others that are known to us from a variety of laboratories.

Mr. ROEMER. Have we narrowed the field down?

Director MUELLER. We are narrowing the field down. But I will also say in the same breath that until we have somebody identified against whom we have brought charges, I would not exclude any possibility. We always keep our minds open for any other possibility. Although the investigation may be leading us down one trail and we may look like we are going in a particular way, we always have to be open to the possibilities of another source of responsibility.

Mr. ROEMER. Is there a time frame on this as to when you hope to conclude it?

Director MUELLER. The chemical analysis will probably be going on for several more months. I would have liked to have concluded it yesterday, I would liked to have concluded it a year ago. And I am comfortable and confident that we are doing everything possible to identify the person responsible for these anthrax attacks.

It is, and I will tell you with the sniper attacks now, it is yet another drain on manpower for this region, but nonetheless, we understand the necessity, the desirability, the importance of doing everything we can to bring the person responsible for those anthrax deaths to justice as soon as possible.

Mr. ROEMER. Do you still believe, to the best of your knowledge, that this is a domestic type of attack with the anthrax or is that still open?

Director MUELLER. Well, the reporters often report what they think we believe.

Mr. ROEMER. You tell me. I will get it straight from you.

Director MUELLER. I have tried not to state what we believe. They have speculated that. I know at one point we had a profile of an individual that we did publish. We have not changed that profile. But I, in the same breath, will tell you that just because the FBI, and they are very good at putting out a profile, a profile is not proof. A profile is not facts indicating a particular person was responsible for that act.

Mr. ROEMER. So you didn't answer my question, and that is okay. But you still don't suspect—you not excluding anything in this? Profile is domestic, but you are not excluding a foreign source or a terrorist source. How about in terms of the sniper case? Do you have any suspicions on that? Your gut? Your personal opinion on this as to what you think?

Director MUELLER. Well I would not—to express——

Mr. ROEMER. George gives that every now and then. He gives his personal opinion.

Director MUELLER. I will tell you at the outset, I believe the investigation is going exceptionally well. There is a combination of the work of state and local coming together in ways that are the way we have to do business in the future. And Charles Moose, the police chief in Montgomery County, is doing superb job and we have a Special Agent in Charge there that is working with him, as does ATF.

Getting to your question as to where the—actually my opinion, I don't think it appropriate that I give you an opinion. What I do think is appropriate is when we have evidence, we present it to the prosecutor so that an arrest can be made.

Mr. ROEMER. But all resources are being devoted. You are confident that everything that the FBI has is being devoted to the case to help the local and State officials pursue this sniper?

Director MUELLER. Not only what the FBI has. As the newspapers reported, to the extent that we believe, with the capabilities, with the Department of Defense we have reached out and sought those capabilities. We will have almost 450 agents who are now participating in that investigation. I believe ATF has close to 200. I don't have a figure myself for the number of state and local law enforcement authorities who are also participating.

I will tell you that we have had thousands of leads, whether it be on our tip line or others, that we are investigating. And there are hopeful leads amongst those that we have received over the last week.

Mr. ROEMER. I thank the Director. I know my time is up. I was hopeful to ask some questions to Mr. Tenet about progress on Usama bin Ladin. But maybe Mr. Reyes will do that.

Mr. REYES. Thank you, Mr. Chairman. Actually I only have one question. I will be glad to yield my time to my colleague. The only question I had was for Mr. Tenet; it was relevant to the testimony on page 9 that you gave where you developed, in 1999, a plan to target Usama bin Ladin and al-Qa'ida globally.

And I am going to assume that the plan includes specific resources, personnel, equipment, training, associated costs. And my question is: Could you furnish us a copy of that plan? I am very much interested in helping the agency on several levels, including on the budget level. So could you furnish that to us?

Director TENET. Yes, sir.

Mr. REYES. Thank you very much. And, I would like to yield my time to——

Mr. ROEMER. Next time the Director is up to our committee, I will ask him about Usama bin Ladin.

Mr. BEREUTER. The gentleman from Oregon, Mr. Wyden.

Senator WYDEN. Director Tenet, as you know, your October 7 letter to Chairman Graham generated a fair amount of discussion. I was interested in asking about a part of it that really hadn't.

The last paragraph in the letter says, and I quote, "Iraq's increasing support to extremist Palestinians, coupled with growing indications of a relationship with al-Qa'ida, suggests that Baghdad's link to terrorists will increase even absent U.S. military action."

Now, I wanted to ask you about this because al-Qa'ida's desire to overthrow secular states and replace them with Islamic governments would threaten Saddam's regime itself. And so my question would be, in your view, and based on the information that you have, what does Saddam gain in the long term by helping al-Qa'ida?

Because the question for me at least—and I would like you to kind of walk us through it—is that a stronger al-Qa'ida puts them in a better position to overthrow his own regime, and al-Qa'ida has a desire to overthrow secular Arab states and threaten them with Islamic governments. And just, if you would, take me through the analysis there.

Director TENET. I actually have a different view. I actually think these distinctions between Sunnis and Shiites and secularists and fundamentalists in the current environment we find ourselves in are bad distinctions to make in terms of looking at behavior for the future.

What do al-Qa'ida and Iraq have in common? Us, the Saudis and others. And the point that I would make to you is, you look at al-Qa'ida and you focus on Iraq or Iran or whoever you want to focus on, but in a clandestine relationship where things are obscured and your hand is hidden, there are enormous advantages.

So I think that distinction that you are making is—now people make that distinction, sir. There are some people who believe it.

Senator WYDEN. I wanted to get your sense of it.

Director TENET. I don't personally buy into it. I actually think we should think about al-Qa'ida as a front company that will take capability wherever it can get it to further its own operational goals, and where there is a confluence of a target that is common and interesting, everybody benefits.

So the letter, in terms of the things that we have seen that we have declassified, senior level contacts, trainings and poisons and gasses among WMD relationships, et cetera, you have seen the letter.

When you peel this story back, I don't know where it is going to take you. And, as is often the case, when you peel the onion back you find more and more all of the time. The only thing I would say is keep your mind open, and don't get—we shouldn't just think about this in conventional terms because they don't think about it that way.

Senator WYDEN. Well, I don't have any quarrel with your analysis. I think that the distinction really is, and you seem to suggest, that these people are just thinking short-term and looking for every possible opportunity, and their short-term interest is to be against the United States, but somehow we have got to reconcile that with some of the long-term considerations as well. That is what I was asking about.

The last point I would make, just as we wrap up these hearings, and I guess I am in a position to be the last to wrap up the public hearings, is that when I look down the road to where we ought to be, it seems that we have to create a new balance. There is a clear need to protect the people of this country, and that requires that sensitive information not be out across the streets of this country.

At the same time, there is a public right to know. And in effect, there is a public need to know, which is what I was trying to address with respect to what I think is the clear over-classification concern that I brought up.

What we are going to try to do up here is to give you all the tools to do it. That is what initiatives like the terrorist identification system that I have developed is a part of. We need you all to meet us halfway. That means getting at the abuses, for example, in the classification area.

I tried to skim over your testimony again. I didn't see the word "classification" come up. Now, I will accept you at your word, because you have been blunt and straight with me in the past that when you say you are going to follow up on it, you do. But this has got to change. I mean, there have been abuses—Pat Moynihan has been talking about that for years.

And I think that what we are talking about is a new balance between ensuring that sensitive information that can't get out, that would threaten this country's wellbeing is protected, but that we also take steps to ensure that the public's right and need to know is addressed, and suffice it to say that is there is a lot of work to do to secure that new balance.

Director TENET. I will work with you, Senator.

Senator WYDEN. Thank you both. Thank you, Mr. Chairman.

Mr. BEREUTER. Thank you. With that, we will conclude the questioning at this hearing. You have heard, the Members have heard and the audience in general has heard the Chairman's plans for the continuation of our effort for the remainder of the 107th Congress.

To you gentlemen, I thank you not only for today but the fact that you have been helping us in closed hearings and otherwise now for some time. And looking at all of the tasks that undoubtedly are upon your desks, hundreds of things, I know the amount of time that we have received from you is substantial.

But what we are doing, of course, in this public hearing and others is maintaining and securing and enhancing the confidence and support of the American people. And I do believe, as I am sure you do, despite the difficulties of maintaining a secure environment in our very open society, that we will prevail, that we will make this country safer for our citizens here and abroad.

Thank you very much, gentlemen. The hearing is concluded.

[Whereupon, at 4:45 p.m., the joint committee was adjourned.]

○