Testimony of
Robert S. Mueller, III
Director
Federal Bureau of Investigation
Before the
Senate Committee on Intelligence of the
United States Senate
February 16, 2005

Introduction

Good afternoon, Mr. Chairman, Senator Rockefeller, and members of the Committee. I appreciate this opportunity to discuss our current view of threats to the United States and the FBI's efforts to address them.

Before I begin, I would like to take a moment to thank all of our partners in the Law Enforcement and Intelligence Communities. They have shared their information and expertise, and in many cases worked side-by-side with us, and together we made great progress over the past year to protect our nation and our communities from terrorism and crime.

I would also like to thank the men and women of the FBI for continuing to embrace our changing mission, for working to enhance our intelligence capabilities, for adapting to new technologies and new ways of doing things, and for doing all of this without ever pausing in our forward push to protect this country from active threats.

Mr. Chairman, over the past year, through unprecedented cooperation, enhanced intelligence capabilities, and continued unwavering commitment to protect the American people, we have achieved considerable victories against national security and criminal threats facing the U.S. However, I must also report that these threats continue to evolve and to pose new challenges to the FBI and our partners.

It remains the FBI's overriding priority to predict and prevent terrorist attacks. The threat posed by international terrorism, and in particular from al Qa'ida and related groups, continues to be the gravest we face.

Al-Qa'ida and Related Terrorist Groups

In 2004, our efforts in the War on Terrorism grew more intelligence-driven, more coordinated, and produced many tangible results.

In 2004 we learned that operatives had conducted detailed surveillance of financial targets in New York, Washington DC, and New Jersey. In response to this threat, in coordination with DHS, the threat level was raised from yellow to orange for the cities referenced in the threat and we mobilized a large contingent of analysts and agents to review the massive amount of information connected with the attack planning, and to uncover any additional information that would give us insight into the plot .

Previously, in the Spring of 2004, our allies in the United Kingdom arrested a group of terrorists who were plotting an imminent attack inside the UK. In response, we immediately formed a task force of analysts and agents to determine if there was a U.S. nexus to the plot or if any of the UK subjects had links to individuals in the U.S.

Later in the year, we received information suggesting that there was an attack being planned -- possibly timed to coincide with the 2004 Presidential Election. To counter the threat, the FBI created the **2004 Threat Task Force** in May 2004. With thousands of FBI personnel, supported by individuals from outside agencies, it was the largest task force created since 9/11, and it brought to bear every possible resource in an effort to identify the operatives and disrupt the attack plan.

As part of the Task Force's initiatives, field offices conducted a thorough canvass of all counterterrorism investigations and FBI sources to develop any further information that could help us find these individuals. During the seven months the task force was up and running, we also checked every tangible lead provided in the threat intelligence. It was an extraordinary effort and while we may never know if an operation was indeed being planned, I am certain that the FBI's tremendous response to the threat played an integral role in disrupting any operational plans that may have been underway.

Mr. Chairman, since we last spoke, the FBI has identified various extremists located throughout the U.S. and is monitoring their activities. Although these efforts have made us safer, they are also a sobering reminder of the threat we continue to face.

- In **Virginia**, Mohammed Ali al-Timimi, the spiritual leader of the Virginia Jihad training group disrupted last year, was indicted for his involvement in the recruitment of US citizens for extremist training and jihad preparation. Al-Timimi, the primary lecturer at a northern Virginia Islamic center, preached jihad to a small core group of followers, provided them paramilitary training and facilitated their travel to Pakistan in the days after September 11th to attend Lashkar-e-Taiba training camp in preparation to fight the United States in Afghanistan
- In **Minneapolis**, we arrested Mohamad Kamal El-Zahabi, a Lebanese citizen who admitted to serving in Afghanistan and Chechnya as a sniper and to providing sniper training at Khalden camp in Afghanistan and in Lebanon in the 1990s. We first learned of El-Zahabi during our investigation of Boston-based Sunni extremists Ra'ed Hijazi, convicted for his role in the Millennium plot in Jordan, and Bassam Kanj, who was killed in a plot to overthrow the Lebanese government in 2000.
- In **New York**, Yassin Muhiddin Aref was arrested on money laundering charges connected to a possible terrorist plot to kill a Pakistani diplomat.

Unfortunately, in spite of these accomplishments, al-Qa'ida continues to adapt and move forward with its desire to attack the United States using any means at its disposal. Their intent to attack us at home remains -- and their resolve to destroy America has never faltered.

Al-Qa'ida's overall attack methodology has adapted and evolved to address the changes to their operating environment. While we still assess that a mass casualty attack using relatively low-tech methods will be their most likely approach, we are concerned that they are seeking weapons of mass destruction including chemical weapons, so-called "dirty bombs" or some type of biological agent such as anthrax.

Every day, personnel in our Counterterrorism Division and in 100 Joint Terrorism Task Forces around the country, work to determine where, when, and how the next attack will occur. The fact remains -- America is awash in desirable targets -- those that are symbolic like the U.S. Capitol and the White House -- as well as the many infrastructure targets, like nuclear power plants, mass transit systems, bridges and tunnels, shipping and port facilities, financial centers, and airports -- that if successfully hit, would cause both mass casualties and a crippling effect on our economy.

We continue to be concerned that U.S. **transportation systems remain a key target**. The attacks in Madrid last March show the devastation that a simple, low-tech operation can achieve and the resulting impact to the government and economy, which makes this type of attack in the U.S. particularly attractive to al-Qa'ida.

Another area we consider vulnerable and target rich is the energy sector, particularly **nuclear power plants**. Al-Qa'ida planner Khalid Sheikh Mohammed had nuclear power plants as part of his target set and we have no reason to believe that al-Qa'ida has reconsidered.

Looking ahead, there are three areas that cause us the greatest concern.

First is the threat from covert operatives who may be inside the U.S. who have the intention to facilitate or conduct an attack. Finding them is a top priority for the FBI, but it is also one of the most difficult challenges. The very nature of a covert operative -- trained to not raise suspicion and to appear benign -- is what makes their detection so difficult.

Mr. Chairman, while we are proud of our accomplishments this year and the additional insight we have gained into al-Qa'ida's activity, I remain **very concerned about what we are not seeing**.

Whether we are talking about a true sleeper operative who has been in place for years, waiting to be activated to conduct an attack or a recently deployed operative that has entered the U.S. to facilitate or conduct an attack, we are continuously adapting our methods to reflect newly received intelligence and to ensure we are as proactive and as targeted as we can be in detecting their presence.

Second, because of al-Qa'ida's directed efforts this year to infiltrate covert operatives into the U.S., **I am also very concerned with the growing body of sensitive reporting that continues to show al-Qa'ida's clear intention to obtain and ultimately use some form of chemical, biological, radiological, nuclear or high-energy explosives (CBRNE) material in its attacks against America**.

Third, we remain concerned about the potential for al-Qa'ida to **leverage extremist groups with peripheral or historical connections to al-Qa'ida, particularly its ability to exploit radical American converts and other indigenous extremists**. While we still believe the most serious threat to the Homeland originates from al-Qa'ida members located overseas, the bombings in Madrid last March have heightened our concern regarding the possible role that indigenous Islamic extremists, already in the U.S., may play in future terrorist plots. Also of concern is the possible role that peripheral groups with a significant presence in the U.S. may play if called upon by members of al-Qa'ida to assist them with attack planning or logistical support.

The potential recruitment of radicalized American Muslim converts continues to be a concern and poses an increasingly challenging issue for the FBI because the process of recruitment is subtle and many times, self initiated and radicalization tends to occur over a long period of time and under many different circumstances.

As part of our continued efforts to identify populations that may be a target for extremist recruitment, the FBI has been involved in a coordinated effort between law enforcement and corrections personnel to combat the recruitment and radicalization of prison inmates. Prisons continue to be fertile ground for extremists who exploit both a prisoner's conversion to Islam while still in prison, as well as their socio-economic status and placement in the community upon their release.

Extremist recruitment at schools and universities inside the United States also poses a particularly difficult problem. Because the environment on campuses is so open and isolated, schools provide a particularly impressionable and captive audience for extremists to target.

Additionally, keeping in mind al-Qa'ida recruitment efforts occur primarily overseas, we are closely monitoring any possible methods for moving individuals to extremist-linked institutions overseas, specifically religious schools and mosques that have overt ties to al-Qa'ida or other terrorist organizations.

We are also concerned about the possibility that individuals who are members of groups previously considered to be peripheral to the current threat, could be convinced by more radical, external influences to take on a facilitation or even worse -- an operational role -- with little or no warning. Individual members of legitimate organizations, such Jama'at Tabligh, may be targeted by al-Qa'ida in an effort to exploit their networks and contacts here in the United States.

Efforts by extremists to obtain training inside the U.S. is also an ongoing concern. Although there are multiple reports and ongoing investigations associated with the paramilitary training activities of suspected extremists nationwide, the majority of these cases involve small groups of like-minded individuals who are inspired by the jihadist rhetoric experienced in radical mosques or prison proselytizing.

Fortunately, the recent amendment to Title 18 adding a provision whereby an individual knowingly receiving military-type training from a designated foreign terrorist organization is committing an offense, makes it possible to now prosecute individuals who participate or assist individuals in receiving this type of training.

Another area of concern is the recent merging of Iraqi jihadist leader Abu Mu'sab al-Zarqawi with al-Qa'ida. Zarqawi has a demonstrated capability of directing external operations while maintaining his focus on Iraq as noted with the disrupted Jordan plot in April.

Another aspect of extremist activity in the U.S. is the extensive fundraising efforts by various terrorist groups. We continue to identify and block funding conduits, freeze assets of terrorists and those who support them, protect legitimate charities, and disrupt the movement of money through peripheral financial systems such as Hawalas.

As part of this effort, the FBI has engaged in extensive coordination with authorities of numerous foreign governments in terrorist financing matters, leading to joint investigative efforts throughout the world. The FBI's participation in a U.S. - Saudi Arabia Joint Terrorism Task Force, the U.S. - Swiss Terrorism Financing Task Force and the International Working Group on Terrorist Financing has enhanced cooperation between these agencies and the U.S. and allowed the FBI unprecedented access that has increased our understanding of these complex financing networks. Since 2002, we have provided terrorism financing training and technical assistance to liaison partners in almost 50 countries.

The Threat from Other International Terrorist Groups

Mr. Chairman, al-Qa'ida and the groups that support it are still the most lethal threat we face today. However, other terrorist groups that have a presence in the U.S. require careful monitoring.

It is the FBI's assessment, at this time, that there is a limited threat of a coordinated terrorist attack in the U.S. from Palestinian terrorist organizations, such as HAMAS, the Palestine Islamic Jihad, and the al-Aqsa Martyr's Brigade. These groups have maintained a longstanding policy of focusing their attacks on Israeli targets in Israel and the Palestinian territories. We believe that the

primary interest of Palestinian terrorist groups in the U.S. remains the raising of funds to support their regional goals.

The FBI is committed to staunching the flow of funds from the U.S. to Palestinian terrorist organizations. As an example of this effort, the former leadership of the Holy Land for Relief and Development, a HAMAS front organization, was indicted this past year and convictions were won against the Elashi brothers who owned and ran Infocom, another HAMAS front organization.

Of all the Palestinian groups, HAMAS has the largest presence in the U.S. with a robust infrastructure, primarily focused on fundraising, propaganda for the Palestinian cause, and proselytizing. Although it would be a major strategic shift for HAMAS, its U.S. network is theoretically capable of facilitating acts of terrorism in the U.S.

Like HAMAS, but on a much smaller scale, U.S.-based Palestine Islamic Jihad members and supporters are primarily engaged in fundraising, propaganda and proselytizing activities. In 2003, the Palestine Islamic Jihad, or PIJ, activities and capabilities in the U.S. were severely undercut by the arrests of the U.S. PIJ leader, Sami al-Arian, and three of his top lieutenants. There have also been two additional arrests of suspected PIJ activists on charges unrelated to terrorism. There has been no indication of a new U.S. PIJ leadership since the arrest of al-Arian.

Currently, the most likely threat of terrorist attacks from Palestinian groups to the U.S. homeland is from a "lone wolf" scenario. In this scenario, a terrorist attack would be perpetrated by one or more individuals who may embrace the ideology of a Palestinian terrorist group, but act without assistance or approval of any established group.

Lebanese Hizballah retains the capability to strike in the U.S., although we have no credible information to indicate that US-based Hizballah members have plans to attack American interests within the U.S. or abroad. In 2004, we had some success in uncovering individuals providing material support to Hizballah.

- In **Detroit**, Mahmoud Youssef Kourani was indicted in the Eastern District of Michigan on one count of Conspiracy to Provide Material Support to Hizballah. Kourani was already in custody for entering the country illegally through Mexico and was involved in fundraising activities on behalf of Hizballah.
- Also in **Detroit**, Fawzi Assi was arrested in May of 2004 and was charged under the 1996 Antiterrorism and Effective Death Penalty Act for providing material support to Hizballah. Assi was initially arrested in 1998 after an outbound US Customs search at the Detroit Metro Airport discovered night vision goggles, one thermal imaging scope and two Boeing Global Positioning System devices. Assi later fled the country after being released by the court on bail but was later turned over to us in Lebanon to face US criminal charges.

The Threat from Domestic Terrorism

While national attention is focused on the substantial threat posed by international terrorists to the homeland, law enforcement officials must also contend with an ongoing threat posed by domestic terrorists based and operating strictly within the U.S. Domestic terrorists motivated by a number of political or social agendas -- including white supremacists, black separatists, animal rights/environmental terrorists, anarchists, anti-abortion extremists, and self-styled militia -- continue to employ violence and criminal activity in furtherance of these agendas.

Animal rights and environmental extremists, operating under the umbrella of the Animal Liberation Front (ALF) and Earth Liberation Front (ELF) utilize a variety of tactics against their

targets, including arson, sabotage/vandalism, theft of research animals, and the occasional use of explosive devices.

Serious incidents of animal rights/eco-terrorism decreased in 2004, a fact we attribute to a series of law enforcement successes that are likely deterring large-scale arsons and property destruction. Following a rash of serious incidents of animal rights/eco-terrorism, including a $50 million arson in San Diego and two bombing incidents in the San Francisco area, law enforcement authorities achieved several significant successes which have likely deterred additional terrorist activity. Despite these successes, we anticipate that animal rights extremism and eco-terrorism will continue to threaten certain segments of government and private industry, specifically in the areas of animal research and residential/commercial development.

The potential for violence by anarchists and other emerging revolutionary groups, such as the Anarchist Black Cross Federation (ABCF), will continue to be an issue for law enforcement. The stated goals of the ABCF are "the abolishment of prisons, the system of laws, and the Capitalist state." The ABCF believes in armed resistance to achieve a stateless and classless society. ABCF has continued to organize, recruit, and train anarchists in the tactical use of firearms.

US-based black separatist groups follow radical variants of Islam, and in some cases express solidarity with al-Qa'ida and other international terrorist groups.

Incidents of organized white supremacist group violence decreased in 2004. This is due to several high profile law enforcement arrests over the last several years, as well as the continued fragmentation of white supremacist groups because of the deaths or the arrests of leaders. We judge that violence on the part of white supremacists remains an ongoing threat to government targets, Jewish individuals and establishments, and non-white ethnic groups.

However, the **right-wing Patriot movement** -- consisting of militias, common law courts, tax protesters, and other anti-government extremists -- remains a continuing threat in America today. Sporadic incidents resulting in direct clashes with law enforcement are possible and will most likely involve state and local law enforcement personnel, such as highway patrol officers and sheriff's deputies.

Potential violent **anti-abortion extremists** linked to terrorism ideologies or groups pose a current threat. The admiration of violent high-profile offenders by extremists highlight continued concerns relating to potential or similar anti-abortion threat activity.

WMD Proliferation and other Foreign Intelligence Threats

Although the impact of terrorism is more immediate and highly visible, espionage and foreign intelligence activity are no less a threat to the US national security. Many countries consider the US to be their primary intelligence target; so long as the US maintains its position in world affairs, it will continue to be targeted. As part of its reinvigorated and refocused foreign counterintelligence (FCI) program, the FBI has applied a more rigorous methodology to its efforts to assess and articulate the current threat environment.

One of the key elements of the FBI's National Strategy for Counterintelligence (adopted in August 2002) is the threat assessment. Over the past two years, the FBI has produced comprehensive threat assessments on several countries deemed to be of particular CI concern. The National Strategy for Counterintelligence identified five categories of foreign intelligence activity as being especially harmful to the US national security. These five categories of activity are weighted in terms of importance, the in the following order:

- Proliferation of chemical, biological, radiological, nuclear, and high-energy explosives (CBRNE) information and technology:
- Penetration of the US Intelligence Community (USIC)
- Penetration of US Government entities and contractors
- Compromise of Critical National Assets (CNAs), defined as any information, policies, plans, technologies, or industries that, if stolen, modified, or manipulated by an adversary would seriously threaten US national or economic security; and
- Conduct of clandestine foreign intelligence activities in the US.

Several countries have traditionally considered the US to be their primary intelligence target, as well as an adversary or threat. This prioritization is manifested through their continued large and active intelligence presence in the US and their aggressive targeting of US persons, information and technology. Other countries, while not necessarily viewing the U.S. as an adversary or threat, seek information to help them compete economically, militarily, and politically in world affairs. As the current leader in all three areas, the US becomes their primary target. For still other countries, rather than being an intelligence target, the US represents an operating environment in which to conduct intelligence-related activities focused on their domestic security.

Some foreign countries are becoming increasingly sophisticated in their CI awareness, training and capabilities. Also of growing concern is the asymmetrical threat posed by certain intelligence services that supplement their collection capabilities in the US by using non-traditional collectors. These collectors include students, delegations, business visitors, émigrés, and retired intelligence officers who are collecting against targets of opportunity or responding to ad hoc requests from the intelligence services. Such non-traditional collectors pose a potential threat across the US, requiring a coordinated response by all FBI field offices.

The FBI does not foresee any significant changes in the official foreign intelligence presence in the US over the next two to three years. However, in addition to using non-traditional collectors, several countries appear to be exploiting their military liaison officers, who are in the US on overt, legitimate intelligence-sharing missions, to target and collect sensitive defense information that is outside the scope of their official access. Most difficult to identify and assess is the intelligence collection activity being directed and/or conducted by non-intelligence organizations, such as other foreign government agencies and/or foreign companies. The FBI sees this type of activity most frequently in the targeting and collection of CBRNE information and technology.

Another challenge the FBI will face is the tendency of some foreign intelligence services to leverage liaison relationships for intelligence collection purposes. US Government representatives participating in international conferences and exchanges, or whose duties include routine liaison with foreign intelligence representatives, frequently report that their contacts engage in elicitation, sometimes to a surprisingly aggressive level.

The FBI expects to see a continued increase in the use of technology as an enabler for intelligence operations, such as contacting, tasking, and debriefing sources and agents in the US.

Over the near term, the priority collection targets for these countries will be:

- The effects of the recent 2004 US elections on US foreign and domestic policies;
- US military actions in Iraq and Afghanistan;

- US counterterrorism policy;
- US dual use technologies; and
- US policy vis-à-vis particular countries or regions of the world.

The FBI expects to see continued lobbying, political influence, and/or perception management activities by countries hoping to affect US policy.

Many foreign intelligence services will also continue to exploit their presence in the US to target and collect against third countries. Most will also engage in defensive intelligence activities, targeting their own expatriate and ethnic communities in the US, especially those groups deemed to be a threat to the current regime.

The FBI's National Strategy for Counterintelligence sets forth national priorities and strategic objectives as well as changes in management and organizational culture intended to redirect and significantly enhance the overall performance of the FBI's FCI program. Program objectives and outcomes include:

- Identify intelligence service objectives, officers, assets, and operations;
- Disrupt the operations of intelligence services; and
- Change the behavior of exploited institutions and individuals.

To that end, the FBI has identified five program strategies: Know the Domain; Understand the Threat; Engage in Strategic Partnerships; Conduct Sophisticated Operations; and Inform Policymakers.

During FY 2004, the FBI FCI program accomplished the following:

- Six foreign intelligence officers and/or agents were arrested;
- 67 requests for persona non grata actions and visa denials were issued;
- 1,667 Intelligence Information Reports were disseminated.

In addition, the Asset Validation Review process was implemented in July 2002, and the FBI began providing mandatory asset validation training for Asset Coordinators in the field regarding procedures and policies. The FBI also implemented the Agents in Laboratories Initiative (AILI) in February 2003, through which FBI agents have been placed in Department of Energy nuclear weapons and science laboratories.

The FBI has also developed several strategic partnerships, to include the Regional CI Working Group (RCIWG) Initiative, which was established in October 2003 to implement the National Strategy for Counterintelligence, leverage the RCIWGs in tasking our USIC partners, address intelligence gaps, identify CI trends and priorities in the operational arena among USIC agencies at the field level, and ensure that all CI operational initiatives and projects across agencies are coordinated through the FBI.

Similarly, the National CI Working Group (NCIWG) was established and is led by the FBI and consists of other CI agency head-level representatives. The mission is to establish ongoing interagency planning discussions to better coordinate CI operations USIC-wide. Domain Task

Forces are CI project level task forces led by the FBI, in vulnerabilities associated with at-risk national security projects, i.e., sensitive technologies, information, and research and development.

FBI field offices are developing "business alliances" to build executive-level relationships and foster threat and vulnerability information sharing, with private industries and academic institutions located within their territories having at-risk and sensitive national security and economic technologies, research and development projects.

Finally, the FBI has reinvigorated its CI training process. For example, field agents are trained in the key components of basic CI operations through an intensive four-week Basic CI Operations course. Other advanced, highly specialized CI courses and seminars provide training to agents and analysts through a variety of innovative instructional methods and include in-services and conferences, the Interactive Multimedia Instruction and Simulation (IMIS) computer-based training program, and the FBI Intranet.

Cyber Threats

The cyber-threat to the U.S. is serious and continues to expand rapidly the number of actors with both the ability and the desire to utilize computers for illegal and harmful purposes rises.

Cyber threats stems from both state actors, including foreign governments that use their vast resources to develop cyber technologies with which to attack our networks, and non-state actors such as terrorist groups and hackers that act independently of foreign governments. The increasing number of foreign governments and non-state actors exploiting U.S. computer networks is a major concern to the FBI and the Intelligence Community as a whole.

State actors continue to be a threat to both our national security as well as our economic security because they have the technical and financial resources to support advanced network exploitation and attack. The greatest cyber threat is posed by countries that continue to openly conduct computer network attacks and exploitations on American systems.

Terrorists show a growing understanding of the critical role that information technology plays in the day-to-day operations of our economy and national security. Their recruitment efforts have expanded to include young people studying mathematics, computer science and engineering in an effort to move from the limited physical attacks to attacks against our technical systems.

Fortunately, the large majority of hackers do not have the resources or motivation to attack the US critical information infrastructures. Most targets of the hacker are viewed as "challenges" to break into a system. These individuals do not introduce malicious code to the system but usually leave their "cyber signature." Although a nuisance, the single hacker does not pose a great threat; however, the increasing volume of hacking activity worldwide does inadvertently disrupt networks, including that of the U.S. information infrastructures. Hackers that plant malicious code or upload bots that are designed to steal information are the main threats in this group. These individuals have the ability to take down a system or steal trade secrets, either of which can be devastating to a company or agency.

The growing number of hackers motivated by money is a cause for concern. If this pool of talent is utilized by terrorists, foreign governments or criminal organizations, the potential for a successful cyber attack on our critical infrastructures is greatly increased.

To combat these and other cyber threats, the FBI established a national cyber program with a Cyber Division at FBI Headquarters and dedicated cyber squads in the field offices. The program enables us to coordinate and facilitate investigations of those federal criminal violations using the Internet, computer systems, or networks. It also helps us to build and maintain public/private

alliances to maximize counterterrorism, counterintelligence, and law enforcement cyber response capabilities. We are also working to aggregate the technological and investigative expertise necessary to meet the challenges that lie ahead. We are recruiting and hiring individuals who possess degrees and experience in computer sciences, information systems, or related disciplines. We are looking for specialists who possess a bedrock of experience and a profound understanding of the cyber world.

Converging Criminal Threats

It is increasingly the case that counterterrorism, counterintelligence, cyber, and criminal investigations are interrelated. There are rarely clear dividing lines that distinguish terrorist, counterintelligence, and criminal activity. Recognizing this trend toward convergence, the first priority of the FBI's Criminal Investigative Program is to leverage criminal investigative resources to enhance the FBI's Counterterrorism, Counterintelligence and Cyber programs.

Terrorists use criminal enterprises and criminal activities to support and fund terrorist organizations. The FBI's criminal investigations of these crimes and criminal enterprises, often in task forces in conjunction with other federal, state, and local law enforcement, continue to develop invaluable intelligence, as well as to initiate investigations, which further identify the United States' vulnerability to attack and directly support the FBI's and the Intelligence Community's counterterrorism, counterintelligence, and cyber crime efforts.

One of the FBI's first investigations to utilize the material support of a terrorist organization statute evolved from a criminal investigation of Hizballah operators utilizing credit card scams, cigarette smuggling and loan fraud to support the purchase of dual use equipment for Hizballah procurement leaders in Lebanon. The FBI used the criminal RICO statute to fully neutralize this terrorist cell.

In combatting converging threats, the FBI's Criminal Program is placing greater emphasis on the collection, analysis, dissemination and effective use of intelligence, including intelligence derived from criminal investigations, including intelligence derived from human sources and the use of sophisticated investigative techniques. We are using intelligence to identify crime problems and trends, to conduct threat assessments, and to drive investigative efforts. Currently, we are aggressively pursuing intelligence collection and threat assessments on Organized Crime, Human Smuggling and Trafficking, Violent Gangs, Public Corruption, Civil Rights, and Middle Eastern Criminal Enterprises.

After CT, CI, and Cyber, the Criminal Investigative Program's other priorities in descending order are Criminal Intelligence, Public Corruption, Civil Rights, Violent Gangs, Criminal Enterprises, Corporate and Securities Fraud, Health Care Fraud, Mortgage Fraud, Major Financial Institution Fraud, and Crimes Against Children and other Violent Crimes.

Public Corruption

Public Corruption continues to pose the greatest threat to the integrity of all levels of government. Recent investigative efforts have been intensified to identify and convict Immigration, Department of State, and DMV officials illegally selling visas or other citizenship documents and drivers licenses to anyone with enough money. Their illegal activities potentially conceal the identity and purpose of terrorists and other criminals, facilitating their entry, travel, and operation without detection in the U.S. Other investigations have convicted numerous law enforcement officers, including those who formed criminal organizations involved in drug trafficking. Many major metropolitan areas in the U.S. have witnessed the indictment and conviction of corrupt public officials who betrayed the public trust for profit or personal gain. Over the last two years alone, the FBI has convicted more than 1050 corrupt government employees, including 177 federal

officials, 158 state officials, 360 local officials, and more than 365 police officers. In addition to pursuing criminal investigations against corrupt law enforcement officers, the FBI has initiated awareness and training efforts to deter corruption, such as "Project Integrity."

Civil Rights

During FY 2004, the FBI initiated 1,744 civil rights investigations and obtained 154 convictions, focusing its efforts on Hate Crimes, Color of Law, and Involuntary Servitude and Slavery matters. The FBI and the United States depend on the support, cooperation and assistance of the Arab, Muslim and Sikh Communities in the United States to fight terrorism and to fight crime. These communities are entitled to the same civil rights of every citizen and person in the United States. The FBI has worked with these communities to ease their fears concerning the FBI's interest in securing their help in the fight against terrorism and to address the backlash of hate crimes directed against them following 9/11 and the war in Iraq. Since 9/11, more than 500 hate crime investigations have been initiated, where the victims were Arab, Muslim, Sikh, or perceived to be as such, resulting in more than 150 federal and local prosecutions. During 2004, the FBI initiated 53 hate crime investigations where the victims were of Arab, Muslim, or Sikh descent or were perceived to be such. Thirteen of those cases resulted in criminal charges being filed by either state or federal law enforcement authorities. Other groups also continue to be the victims of Hate Crimes, including African American and Jewish communities.

Human trafficking and modern day slavery are a worldwide crime and human rights problem, due to global, economic, and political factors. Approximately 17,000 victims each year are lured to the United States with false promises of good jobs and better lives and then forced to work under brutal and inhumane conditions. Many trafficking victims, including women and children, are forced to work in the sex industry, prison like factories, and migrant agricultural work.

Violent Gangs

Violent gangs are more organized, larger, more violent, and more widespread than ever before, and they pose a growing threat to the safety and security of Americans. The Department of Justice estimates there are approximately 30,000 gangs with more than 800,000 members in the U.S.

Our communities continue to experience devastating incidences of murder, drive-by shootings, and assaults by gangs mainly involved in the sale and distribution of illicit drugs. However, gang activity extends far beyond protection of turf. It impacts innocent citizens who have no connection or involvement with gangs, and it increasingly transcends municipal boundaries. Gang members travel from city to city, between states and, on occasion, between countries to commit their crimes.

In response, the FBI is implementing a coordinated, intelligence-driven National Gang Strategy to disrupt and dismantle gangs that pose the greatest threats to America's communities. In the past year, we have increased the number of Safe Street Task Forces from 78 to 107 and we are seeking to increase the number by an additional 10 to 20 percent in the coming year. We are also centralizing gang investigations at FBI Headquarters with a new $10 million National Gang Intelligence Center (NGIC). The NGIC will collect intelligence on gangs from across the U.S., analyze this intelligence, and disseminate it to help law enforcement authorities throughout the country plan and execute strategies to prevent further gang activity and violence.

The FBI has reclassified gang matters from "violent criminal offenders" to "criminal organizations and enterprises" -- a higher priority area. The new classification also allows the U.S. Department of Justice to charge gang members under federal racketeering statues which can result in stiffer

prison sentences for convicted subjects. This approach is similar to the successful strategy used by the FBI to dismantle traditional organized crime groups.

Under the National Gang Strategy, priority is given to efforts to disrupt and dismantle gangs that are national in their scope and exhibit significant connectivity and internal alliances. Among the first to be targeted is Mara Salvatrucha (MS-13), a violent gang which originated in Los Angeles comprised primarily of Central American immigrants. We have created a National Gang Task Force specifically to address MS-13.

Criminal Enterprises

Organized criminal enterprises operating in the U.S. and throughout the world pose increasing concerns for the international law enforcement and intelligence communities. Their skill in using international monetary systems to conduct and conceal their criminal activity, their use of state of the art communications encryption to further safeguard their illegal activity, and their transnational mobility increases the likelihood they will escape detection or otherwise cover their illegal activities with a cloak of legitimacy. Although the FBI prioritizes its efforts on criminal enterprises with possible connections to terrorist and counterintelligence activities, public corruption, human smuggling of Special Interest Aliens and women and children, or violent and pervasive racketeering activity, the impact from just one criminal activity alone, theft, is staggering. Annual property losses from cargo/high tech/retail theft is estimated at $30 billion, from vehicle theft $8 billion, from art/cultural heritage artifact theft $500 million, and from jewelry and gem theft $135 million. However, theft by criminal enterprises often represents a multifaceted threat. For example, Middle Eastern Criminal Enterprises involved in the organized theft and resale of infant formula pose not only an economic threat, but a public health threat to infants, and a potential source of material support to a terrorist organization.

The FBI is increasing its intelligence collection and assessment efforts on criminal enterprises, as well as its joint efforts with the intelligence and law enforcement services of other nations, to combat the criminal activities of the La Cosa Nostra, Italian, Russian, Balkan, Albanian, Asian, African, Middle Eastern, Colombian/South American and other criminal enterprises. The FBI/Hungarian National Bureau of Investigation Organized Crime Task Force in Budapest, Hungary, which is investigating a Russian Criminal Enterprise engaged in murder, extortion, prostitution, and other significant racketeering activity, represents an unprecedented cooperative effort between the FBI and the Hungarians.

Although new criminal enterprises continue to emerge, the LCN remains a formidable and ever changing criminal threat. This year, in just one criminal scheme, identified by the Federal Trade Commission as the largest consumer fraud investigated in the history of the United States, members of the Gambino LCN family were convicted for using pornographic websites and adult entertainment 1 800 numbers to defraud thousands of individuals of $750,000,000. Asian Criminal Enterprises also pose a continued threat, as exemplified by one which was dismantled earlier this year during a coordinated arrest operation with Canada, which resulted in the arrest of 36 subjects in Canada and 102 subjects in the U.S. for drug trafficking and money laundering. Millions of dollars and 21 firearms, including an AK 47 assault rifle and a sawed off shotgun were seized during the operation.

Corporate/Securities Fraud

Corporate fraud can cost Americans their jobs and rob them of hard-earned savings. It shakes the public's confidence in corporate America to its foundation. Since the initiation of the FBI Corporate Fraud Task Force in December 2001, there have been 480 indictments and 305 convictions of corporate executives and their associates. The FBI's efforts have also resulted in over $2 billion in restitutions, recoveries and fines, in addition to over $30 million in seizures and

forfeitures. In the Enron, HealthSouth, Cendant Corporation, Credit Suisse First Boston, Computer Associates International, Worldcom, Imclone, Royal Ahold, Perigrine Systems, and America On Line cases the FBI obtained 119 indictments/ informations and 79 convictions. The former Chief Executive Officer (CEO) of Worldcom is on trial in New York and the former CEO of HealthSouth is on trial in Alabama. Several additional high profile trials are anticipated in the near future, to include the trial of Enron's former CEOs and Chief Accounting Officer anticipated to be scheduled for August or September 2005.

The FBI is currently pursuing 334 Corporate Fraud cases throughout the U.S. This is more than a 100 percent increase from FY 2003. Eighteen of the pending cases involve losses to public investors which each exceed $1 billion. Unfortunately, the volume of cases has yet to reach a plateau, and the FBI continues to open three to six new cases each month, each case averaging a loss exceeding $100 million.

Health Care Fraud

American's health care expenditures continue to climb at rates higher than inflation and will soon consume more than 17 percent of the Gross Domestic Product. It is estimated that health care fraud costs consumers, Medicare, Medicaid, and private insurers tens of billions of dollars each year in blatant fraud schemes in every sector of the industry. The FBI recently instituted the Out Patient Surgery and Pharmaceutical Fraud Initiatives to combat blatant fraud identified in those health care programs. During FY 2004, the FBI had 2,468 pending health care fraud investigations, obtained 693 indictments and informations, 564 convictions or pre trial diversions, $1.05 billion in restitution, $543 million in fines, $28.8 million in seizures, $19.05 million in forfeitures and disrupted 186 and dismantled 105 criminal organizations.

Mortgage Fraud

The number of FBI mortgage fraud investigations, including major undercover operations, rose from 102 in FY 2001 to approximately 550 in FY 2004. This rise is expected to continue. During FYs 2001-2004 the FBI received over 17,000 mortgage fraud related Suspicious Activity Reports from federally insured financial institutions alone. The FBI worked with the Mortgage Bankers' Association (MBA), the National Notary Association (NNA), as well as FINCEN, the Department of Housing and Urban Development, and major mortgage lending institutions, to improve the reporting and detection of potential mortgage fraud.

Crimes Against Children/Violent Incident Crime

Of all violent crime, crimes against children and child prostitution are of particular concern. Over 300,000 children per year are forced into prostitution. The FBI's Lost Innocence, Child Prostitution Initiative, has opened 13 cases in 11 field offices, emphasizing the use of sophisticated investigative techniques, to obtain 135 arrests/locates, 3 complaints, 13 indictments/informations, 11 convictions/pre trial diversions, and 4 child locates. Major violent crime incidents, such as sniper murders, serial killings and child abductions can paralyze whole communities and require the cooperative efforts of the FBI and local, state and other federal law enforcement agencies. The FBI also continues to address the 6,218 bank robberies, resulting in 153 injuries, and 15 deaths, that occurred within the first ten months of 2004, albeit with a greater reliance on other agencies and a lesser use of its own resources where possible.

Enhancing the FBI's Capabilities

Mr. Chairman, you will notice that our accomplishments over the past year consistently have two things in common, the effective collection and use of intelligence and inter-agency cooperation. The improvements that made these accomplishments possible result from the continued efforts of

the men and women of the FBI to implement a plan that fundamentally transforms our agency and enhances our ability to predict and prevent terrorism.

Intelligence

As set forth above, threat information crosses both internal and external organizational boundaries. Counterterrorism efforts must draw from, and contribute to, counterintelligence, cyber and criminal programs. In order to most effectively address all threats, we are continuing to strengthen the FBI's enterprise-wide intelligence program.

We began in 2001 with a dedicated analysis section in the Counterterrorism Division and, in 2002, we created an Office of Intelligence in the Counterterrorism Division. The structure and capability significantly enhanced our CT operations and those of our partners. In 2003, we extended this concept across all FBI programs -- Criminal Cyber, Counterterrorism and Counterintelligence-and unified intelligence authorities under a new FBI Office of Intelligence led by an Executive Assistant Director. The Office of Intelligence adopted Intelligence Community best practices to direct all FBI intelligence activities. Congress and the 9/11 Commission reviewed these efforts and provided recommendations to further strengthen the FBI's intelligence capability.

The newly established Directorate of Intelligence is the dedicated national security workforce that the Congress established within the FBI. It comprises a dedicated Headquarters element and embedded intelligence entities in each FBI field office called Field Intelligence Groups (FIGs). The FIGs are central to the integration of the intelligence cycle into field operations. The FIGS include Special Agents, Intelligence Analysts, Language Specialists, and Surveillance Specialists, as well as officers and analysts from other intelligence and law enforcement agencies. They are responsible for coordinating, managing, and executing all of the functions of the intelligence cycle and have significantly improved the FBI's intelligence capability. This integrated intelligence service leverages the core strengths of the law enforcement culture -- such as reliability of sources and fact-based analysis -- while ensuring that no walls exist between collectors, analysts and those who must act upon intelligence information. The Directorate also benefits from the strong FBI history of joint operations by unifying FBI intelligence professional and integrating all partners, particularly state, local, and tribal law enforcement, into our intelligence structures.

The central mission of the Directorate is to optimally position the FBI to meet current and emerging national security and criminal threats by: (1) assuring that the FBI proactively targets threats to the US, inhibiting them and dissuading them before they become crimes; (2) providing useful, appropriate and timely information and analysis to the national security, homeland security, and law enforcement communities; and (3) building and sustaining FBI-wide intelligence policies and capabilities.

In 2004, we made substantial progress to expand and strengthen our intelligence workforce. For the first time, the FBI offered recruitment bonuses for Intelligence Analysts. As a result of these and other efforts, the FBI received over 80,000 applications and hired over 650 Intelligence Analysts.

We built on the College of Analytic Studies, created in October 2001, with the addition of two new courses based on intelligence community best practices: ACES 1.0, a new basis intelligence analytic course, and ACES 1.5, a course for experienced, on-board analysts that provides information on the latest analytic resources and techniques. To ensure a consistent level of knowledge across the workforce on intelligence concepts and processes, ACES Training is now mandatory for all FBI Intelligence Analysts. We have increased our training expertise and capacity and are on track to deliver basic training to 1,000 Intelligence Analysts by December 2005. In addition, we have incorporated intelligence training into New Agents class, including a joint exercise with Intelligence Analysts and joint evening seminars.

The Intelligence Analyst career path, with multiple work roles and cross-training requirements not only provides career development opportunities, it also creates a workforce with the agility and flexibility needed to respond to the changing threat environment.

In addition, we implemented several initiatives to enhance the analyst career path and improve retention. We extended the promotion potential for analysts in the field from GS-12 to GS-14. We created an Intelligence Analyst Advisory Board, leveraging the strong FBI culture of creating advisory groups to provide advocacy for specific career fields. At the same time we worked with Congress and were granted pay flexibilities, such that FBI intelligence professionals now can be compensated at a rate equal to that of their Intelligence Community peers. These and other initiatives have helped us to stabilize our attrition rate between 8 percent and 9 percent and FY05 statistics to date look promising.

We have also taken steps to strengthen the Special Agent component of our intelligence workforce. In March 2004 we established a new career path for Special Agents with three objectives. First, the career path gives all Agents experience in intelligence collection, analysis and dissemination. Second, the career path will give Agents an opportunity to develop specialized skills, experience and aptitudes in one of four areas: 1) Intelligence, 2) Counterterrorism/Counterintelligence, 3) Cyber or 4) Criminal. Third, it makes Intelligence Officer Certification a prerequisite for advancement to senior supervisory ranks. The Special Agent career path will produce a cadre of Agents who are proficient in both intelligence and law enforcement operations. This is key to achieving the full integration of law enforcement and intelligence operations.

To improve our foreign language capabilities, we have recruited and processed more than 50,000 translator applicants. These efforts have resulted in the addition of 778 new Contract Linguists (net gain of 493 after attrition) and 109 new Language Analysts (net gain of 34 after attrition). The FBI has increased its overall number of linguists by 67%, with the number of linguists in certain high priority languages increasing by 200% or more.

We have integrated management of the FBI's Foreign Language Program (FLP) into the Directorate of Intelligence. This integration fully aligns FBI foreign language and intelligence management activities and delivers a cross-cutting platform for future improvements across all program areas, including translation quality controls.

We also established the Language Services Translation Center (LSTC), a command and control structure at FBI Headquarters to ensure that our finite translator resource base of over 1,300 translators, distributed across 52 field offices, is strategically aligned with priorities set by our operational divisions on a national level.

We have built a secure network that allows us to efficiently route FISA audio collection to any FBI field office. This technology allows us to more effectively utilize our national translator base.

We now possess sufficient translation capability to promptly address all of our highest priority counterterrorism intelligence, often within 12 hours. Of the several hundred thousand hours of audio materials and several million pages of text collected in connection with counterterrorism investigations over the last two years, a nominal level of backlog exists only because of obscure languages or dialects.

We have instituted a national translation quality assurance program. Countervailing operational pressures, however, limit our ability to fully comply with instituted translation review procedures in those languages for which demand continues to outpace supply. In those languages for which we have already achieved excess translation capacity, e.g., Farsi, Pashto, and Vietnamese, 100% quality assurance compliance is expected by April 2005.

Translation backlogs continue to exist within our counterintelligence program. To target these deficiencies, we have implemented a highly successful workforce planning model which links field-wide workload measurements, trend analysis, and geo-political indicators to our recruitment and applicant processing efforts.

In 2005, we plan to strengthen the integration of the entire intelligence cycle (requirements management; planning and direction; collection; processing and exploitation of collected information; analysis and production; and dissemination) into field office operations.

We will incorporate the recently-developed new critical element entitled, "Intelligence," into the performance plans of all Special Agents and Supervisory Special Agents; this new element emphasizes participation in intelligence cycle functions, in particular human source development and contributions to intelligence production.

We will also establish "fly-teams" of Agents with intelligence experience, Intelligence Analysts, Language Specialists, and Surveillance Specialists to travel to five field offices and provide hands-on guidance and training for the full integration of the intelligence cycle within the office.

Partnerships

Our ability to coordinate and communicate with other members of the Intelligence Community has never been better. Our face-to-face interaction with the National Counterterrorism Center and members of the CIA and DHS has positively impacted our ability to come together on a common problem and the results of the cooperation are evident. Case in point: during the election threat, analysts were able to meet daily to discuss assessments and develop theories that were fundamental to understanding the threat, and from those meetings, on-line forums were created to facilitate continued sharing of ideas and new intelligence finds -- all from the desktop.

The FBI's Information Sharing Policy Group, chaired by the FBI's EAD-Intelligence, brings together the FBI entities that generate and disseminate law enforcement information and intelligence to implement the FBI's goal of sharing as much as possible consistent with security and privacy protections.

Within the Intelligence Community, the FBI has a two-level approach:

22. For those agencies that operate at the Top Secret-SCI level, we are investing in secure facilities for an FBI network (SCI On-Line, or SCION) that is linked to the DOD-based JWICS network used by CIA, NSA, and other national agencies.
23. For those agencies that operate at the Secret level, we have connected the FBI's internal electronic communications system to the DoD-based SIPRNET network that serves. As a result, all FBI Agents or analysts who need to communicate at the Secret-level with other agencies can do so from their desktop.

Within the law enforcement community, the FBI's National Information Sharing Strategy (NISS) is part of the DOJ Law Enforcement Information Sharing Program and builds upon the FBI Criminal Justice Information (CJIS) Services program.

24. The Law Enforcement National Data Exchange (N-DEx) will provide a nationwide capability to exchange data derived from incident and event reports. Data from incident and arrest reports -- name, address, and non-specific crime characteristics -- will be entered into a central repository to be queried against by future data submissions. The national scale of N-DEx will enable rapid coordination among all strata of law enforcement.

25. The Law Enforcement Regional Data Exchange (R-DEx) will enable the FBI to join participating Federal, state, tribal, and local law enforcement agencies in regional full-text information sharing systems under standard technical procedures and policy agreements.
26. The FBI makes national intelligence more readily available to state, tribal, and local law enforcement agencies through the Law Enforcement Online (LEO) network.
27. The Terrorist Screening Center (TSC) also leverages the CJIS backbone to provide real-time actionable intelligence to state and local law enforcement.

Information Technology

Recognizing that the ability to assemble, analyze and disseminate information both internally and with other intelligence and law enforcement agencies is essential to our success in the war on terrorism, the FBI has made modernization of its information technology (IT) a priority.

Under the centralized leadership of the Chief Information Officer (CIO), the FBI is now taking a coordinated, strategic approach to IT. We have a Strategic IT Plan, a baseline Enterprise Architecture, and a system for managing IT projects at each stage of their "life cycle" from planning and investment, through development and deployment, operation and maintenance, and disposal. This involves regular technical reviews to see if milestones are met.

The first two phases of the Trilogy IT modernization program have been completed. The FBI is now modernized with:

28. Deployment of a high-speed, secure network that enables personnel in FBI offices around the country to share data, including audio, video and image files.
29. More than 30,000 new desktop computers with modern software applications 3,700 printers, 1600 scanners, 465 servers and 1400 routers.
30. An IT infrastructure that provides for secure communication with our Intelligence Community partners.

The third phase of Trilogy, which includes the Virtual Case File (VCF) has not yet been completed. Plans for VCF have changed both in response to identified technical problems and because the FBI's refocused mission created requirements that did not exist when VCF was originally envisioned, such as requirements related to information sharing. Last June, after we determined that the product delivered did not meet our needs, we decided to move forward with a two-track action plan for VCF.

31. In accordance with this plan, we asked a new contractor to examine the latest working version of the VCF as well as available off-the-shelf software applications and those designed for other agencies, to determine the best combination to meet the FBI's needs. In many ways, the pace of technological innovation has overtaken our original vision for VCF, and there are now existing products to suit our purposes that did not exist when Trilogy began.
32. As we move forward, we will apply all that we have learned and leverage what we have already developed, including a critical interface to our existing data systems that will be a key component of our final solution.

Separate from the Trilogy Program, we have successfully developed and deployed a number of new investigative and information sharing capabilities.

The **Investigative Data Warehouse (IDW)** offers Agents and analysts alike the technology to perform link analysis, while also providing enhanced search and analytical tools. IDW provides FBI users with a single access point to more than 47 sources of counterterrorism data, including information from FBI files, other government agency data, and open source news feeds, that

were previously available only through separate, stove-piped systems. Most of these users are with the Directorate of Intelligence, Counterterrorism or Counterintelligence Divisions. These users provide search and analysis services using the IDW for personnel throughout the Bureau.

The **FBI Automated Messaging System (FAMS)** began operations in December and now provides more than 300 users with the capability to send and receive critical organizational message traffic to any of the 40,000+ addresses on the Defense Messaging System (DMS). The FBI is the first civilian agency to operate a classified DMS.

The **FBI Intelligence Information Reports Dissemination System (FIDS)** is a web-based software application that allows all FBI personnel with access to the FBI's Intranet to create and disseminate standardized Intelligence Information Reports (IIRs) quickly and efficiently. FIDS allows the Directorate of Intelligence to automate and standardize IIR creation and dissemination functions.

Conclusion

Looking forward, we expect certain trends to continue. Our adversaries will keep evolving, national security and criminal threats will further converge, and old jurisdictional boundaries will become less and less relevant. If we are to address these trends successfully, we must be willing and able to evolve ourselves. The FBI must continue to build our intelligence capabilities, including a strong intelligence workforce. We must continue hiring and training personnel with technical expertise and foreign language skills. We must continue to seek new ways to share information and collaborate with partners in the Intelligence and Law Enforcement Communities. Above all, we must be agile, and encourage creativity, innovation, and strategic thinking. If we do all of these things, I am confident that we will out-network, out-think, and ultimately defeat our adversaries.

Mr. Chairman, I thank you again for this opportunity. I look forward to working with this committee as we continue our efforts to address threats to the U.S. I would be happy to take any questions you might have.

http://www.fbi.gov/congress/congress05/mueller021605.htm