Order Code RL32597

CRS Report for Congress
Received through the CRS Web

Information Sharing for Homeland Security: A Brief Overview

Updated September 30, 2004

Harold C. Relyea
Specialist in American National Government
Government and Finance Division

Jeffrey W. Seifert
Analyst in Information Science and Technology Policy
Resources, Science, and Industry Division

Information Sharing for Homeland Security: A Brief Overview

Summary

In the aftermath of the terrorist attacks on the World Trade Center and the Pentagon, various recommendations and efforts have been made with the intention of improving information sharing among government entities at all levels within the United States, the private sector, and certain foreign governments, with a view to countering terrorists and strengthening homeland security. The National Commission on Terrorist Attacks Upon the United States (9/11 Commission) is among those to have most recently offered recommendations in this regard in its July 22, 2004, report. The types of information potentially within the scope of such sharing include raw data, which has undergone little or no assessment regarding its accuracy or implications; knowledge, which has been determined to have a high degree of reliability or validity; and intelligence, which has been carefully evaluated concerning its accuracy and significance, and may sometimes be credited in terms of its source. This report reviews some of the principal existing homeland security information sharing arrangements, as well as some projected arrangements in this regard, and discusses related policy, evaluations, and proposed legislation (H.R. 10, H.R. 5024, S. 2774/H.R. 5040, S. 2845/H.R. 5140). It will be updated as events warrant.

Contents

Information Sharing for Homeland Security: A Brief Overview

Among the responses prompted by the terrorists attacks on the World Trade Center and the Pentagon were various recommendations for, and subsequent efforts at, improving information sharing among government entities at all levels within the United States, the private sector, and certain foreign governments, with a view to countering terrorists and strengthening homeland security. The National Commission on Terrorist Attacks Upon the United States (9/11 Commission) is among those to have most recently offered recommendations in this regard in its July 22, 2004, report. Because the commission's report arrived at a time when information sharing improvements were well underway, its recommendations are multifaceted.

9/11 Commission Recommendations

In Chapter 12, titled "What to Do? A Global Strategy," the commission's report provided two sets of recommendations pertaining to the exchanging or sharing of information. With respect to border screening, the panel proffered the following recommendation:

- **The U.S. government cannot meet its own obligations to the American people to prevent the entry of terrorists without a major effort to collaborate with other governments. We should do more to exchange terrorist information with trusted allies, and raise U.S. and global border security standards for travel and border crossing over the medium and long term through extensive international cooperation.**[1]

While the commission's recommendation was not specific as to how such collaborations could be carried out, the report suggested the need for global standards for identity authentication (such as biometrically enhanced passports), and stated that the U.S. should take a leading role in establishing these standards. One potential longer term implication of carrying out this recommendation is a global network of country-based screening systems that could verify the departure/arrival of an individual and authenticate that person's identity in real time.

While advocating greater information sharing, the report also recognized how consolidating and transferring large amounts of information about individuals could be susceptible to abuse. Regarding the protection of civil liberties, the report called for an "enhanced system of checks and balances" to be built into the policy framework used to oversee and regulate information sharing. To that end, three

---

[1] U.S. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington: GPO, 2004), p. 390.

recommendations were included regarding what information would be shared, why the information would be shared, and who would be overseeing these activities.

- **As the President determines the guidelines for information sharing among government agencies and by those agencies with the private sector, he should safeguard the privacy of individuals about whom information is shared.**

- **The burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use.**

- **At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties.**[2]

In Chapter 13, titled "How To Do It? A Different Way of Organizing Government," the commission's report included two recommendations that explicitly address the need to facilitate the development of a *policy* and *technical* environment that encourages and supports information sharing. With respect to developing policies that foster a culture of information sharing, the commission recommended:

- **Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge.**[3]

This commission recommendation highlighted what it considered to be a significant impediment to comprehensive intelligence analysis — the "'need-to-know' culture of information protection."[4] The commission suggested that, while the federal government has access to huge volumes of information, procedural and organizational cultural barriers undermine the government's ability to capitalize on these resources. The commission also cited two specific factors that have helped to perpetuate "need-to-know" information practices. One is the lack of robust internal information sharing procedures, which, in turn, has contributed to the compartmentalization of information as a standard practice, rather than the regular dissemination of information to the external community of users. According to the commission, current procedures allowed information to be shared if someone specifically requested the information, and then only according to classification and other security protocols. The purpose of such an approach is to guard against the

---

[2] Ibid., pp. 394-395.

[3] Ibid., p. 417.

[4] Ibid.

disclosure of information that could create security risks. However, the commission suggested that, if taken too far, such security procedures can outweigh the benefits that could be gleaned from information sharing.[5]

A second factor cited by the commission as perpetuating "need-to-know" information practices is an organizational culture, prevalent across agencies, that supports disincentives to information sharing. As the report states: "There are no punishments for *not* sharing information."[6] However, depending upon the situation, criminal, civil, and/or administrative penalties can be imposed if information is shared or disclosed in violation of procedure. The commission suggested that the emphasis on security had led to the "overclassification and excessive compartmentalization of information among agencies."[7] Obstructed access to information can also have both analytical and financial costs, by contributing to incomplete analysis and the duplication of effort by various agencies.

To address these concerns, the commission advocated replacing the "need-to-know" information culture with a "need-to-share" information culture. In order to transition to an intelligence information environment that emphasizes the "need-to-share," development of new procedures must also be matched with the development of a technical infrastructure that enables actual information sharing. To that end, with respect to developing the technical infrastructure for information sharing, the commission offered the following recommendation:

- **The president should lead the government-wide effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy, and technical issues across agencies to create a 'trusted information network.'"**[8]

The report did not specify exactly how a trusted information network would be constructed, who would use it, or what information would be shared through it. However, it did highlight some of key features that would characterize the trusted information network, and cited an example described in a recent Markle Foundation report as "an outstanding conceptual framework for the kind of 'trusted information network.'"[9] According to the commission's report, the trusted information network would be based on a decentralized network model that would facilitate information sharing not only within agencies (vertically), but also, more critically, across agencies (horizontally). The report also recommended using a digital rights management framework, so that a trusted information network could allow agencies to maintain

---

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid., p. 418.

[9] Ibid.; the Markle Foundation report, produced in December 2002 by its Task Force on National Security in the Information Age, is titled *Creating a Trusted Information Network for Homeland Security: Second Report of the Markle Foundation Task Force*, and is available at [http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf].

and populate their own databases, as well as establish access controls to govern the use of the data by authorized individuals within the network. The commission also suggested that presidential leadership would be required to address the policy and legal issues associated with establishing a trusted information network. This leadership, in turn, could develop standards for common information use, and could be applied across the participant community.

Another recommendation would have the President, when determining "the guidelines for information sharing among government agencies and by those agencies with the private sector," also "safeguard the privacy of individuals about whom information is shared." Seeking to reinforce compliance with these guidelines, and otherwise finding "that there is no office within the government whose job it is to look across the government at the action we are taking to protect ourselves to ensure that liberty concerns are appropriately considered" the report recommended the creation of the civil liberties oversight board proposed in Chapter 12.[10]

On August 27, 2004, President George W. Bush issued two executive orders responding to some of these recommendations of the 9/11 Commission. One of them, E.O. 13356, prescribed duties for the heads of agencies possessing or acquiring terrorist information concerning the accessibility, sharing, and analysis of such information; set requirements for the collection of terrorism information within the United States; and, among other considerations, established an Information Systems Council, chaired by a representative of the Director of the Office of Management and Budget (OMB) with at least 10 other members representing specified senior officials, "to plan for and oversee the establishment of an interoperable terrorism information sharing environment to facilitate automated sharing of terrorism information among appropriate agencies."[11]

The other directive, E.O. 13353, established the President's Board on Safeguarding Americans' Civil Liberties within the Department of Justice.[12] Chaired by the Deputy Attorney General and composed of 19 other senior counsels and leaders largely from within the intelligence and homeland security communities, the board may advise the President regarding civil liberties policy, gather information and make assessments regarding such policy and its implementation, make recommendations to the President, refer information about possible violations of such policy by a federal official or employee for prompt action, enhance cooperation and coordination among federal departments and agencies in implementing such policy, and undertake other efforts to protect the civil liberties of the citizenry as the President may direct.

In the paragraphs below, some of the principal existing homeland security information sharing arrangements are reviewed, as well as some projected arrangements in this regard; and related policy, Government Accountability Office (GAO, formerly known as the General Accounting Office) evaluations, and

---

[10] Ibid., p. 394-395.

[11] *Federal Register*, vol. 69, Sept. 1, 2004, pp. 53599-53602.

[12] Ibid., pp. 53585-53587.

legislation are discussed. The types of information potentially within the scope of such sharing include raw data, which has undergone little or no assessment regarding its accuracy or implications; knowledge, which has been determined to have a high degree of reliability or validity; and intelligence, which has been carefully evaluated concerning its accuracy and significance, and may sometimes be credited in terms of its source.

Existing Arrangements

While discussions of information sharing frequently focus on how technology can be used to break down the so-called "stove pipes" that purportedly inhibit collaboration among government agencies, it is important to recognize that these initiatives are more than simply information technology projects. Instead, they represent a specific component of ongoing efforts to improve the management, efficiency, and efficacy of government information resources, often associated with electronic government (e-government). As such, information sharing initiatives are characterized by their programmatic elements as well as their technology elements. Some of the most common categories or types of information being shared through these initiatives include intelligence, homeland security, law enforcement, and critical infrastructure information.

Information shared and technology used by these initiatives can vary widely. However, an overarching purpose of most of these initiatives is to facilitate better collaboration and information analysis through the use of improved information technology and the development of common information standards. Concerns about coordination and duplication of these initiatives have been raised since there currently appears to be no centralized inventory of all the information sharing initiatives being carried out within and between the federal, state, and/or local levels.[13] GAO has reported, however, that efforts to fight terrorism have spurred the growth of the number of initiatives at all levels of government since the September 11, 2001, attacks.[14] Three existing information sharing initiatives are discussed below to provide general examples of how information sharing is sometimes carried out.

Joint Regional Information Exchange System (JRIES) and the Homeland Security Information Network (HSIN). In December 2002, JRIES began as a pilot project for the sharing of counterterrorism information between local and state law enforcement and the Department of Defense (DOD). JRIES was initiated by the Joint Intelligence Task Force - Combating Terrorism (JITF-CT), led by the Defense Intelligence Agency (DIA). The initial participants included the New York Police Department Counterterrorism Bureau (NYPD-CTB) and the California Department of Justice Anti-Terrorism Information Center (CATIC). After assessment of the pilot phase, JRIES became operational in February 2003. The

---

[13] See U.S. General Accounting Office, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO Report GAO-03-760 (Washington: August 2003).

[14] Ibid.

number of participants has also grown to include other municipalities, states, and federal agencies.[15]

In February 2004, the Department of Homeland Security (DHS) announced the launch of its Homeland Security Information Network (HSIN) initiative, designed to connect all 50 states, five U.S. territories, and 50 major urban areas with the Homeland Security Operations Center (HSOC) at the department. To accomplish this goal, DHS adopted the JRIES infrastructure, expanding both its capabilities and its community of users beyond its original "law enforcement and intelligence counterterrorism mission" while leaving the original JRIES system in place.[16] In July 2004, DHS announced that it achieved connectivity to all 50 states.[17] JRIES/HSIN is anticipated to include eventually users such as state homeland security advisers, state adjutant generals (National Guard), state emergency operations centers, local emergency services (fire, police, and other first responders), and possibly private sector actors as well. A significant focus of the expanded JRIES/HSIN network will be to prevent terrorist attacks by capitalizing on the existing human and information resources at the federal, state, and local levels, and enabling the real time collaboration and exchange of information for improved awareness and quicker response to threats.[18] Some civil liberties organizations have raised concerns regarding the exchange of information by state and local law enforcement agencies with DIA, an intelligence agency barred from collecting information domestically. Concerns also have been raised about the potential collection information regarding the activities of legitimate political or social organizations, such as anti-war groups.[19]

JRIES functions as a secure virtual private network (VPN), connecting various participant data sources using encrypted communications via the Internet. JRIES relies upon commercial, off-the-shelf technology and Web-based software that enables users to access database and analysis applications, send secure e-mail, send and receive maps and other graphics, and collaborate in real time online.[20] JRIES/HSIN is currently used to exchange so-called sensitive but unclassified (SBU)

---

[15] U.S. Department of Justice, Office of Justice Programs, *The National Criminal Intelligence Sharing Plan* (Washington: October 2003), pp. 45-56, available at [http://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf].

[16] U.S. Department of Homeland Security, "Homeland Security Information Network to Expand Collaboration, Connectivity for States and Major Cities," press release, Feb. 24, 2004, available at [http://www.dhs.gov/dhspublic/display?content=3350].

[17] Dibya Sarkar, "HSIN Starts Five Months Early," *Federal Computer Week*, July 8, 2004, available at [http://www.fcw.com/fcw/articles/2004/0705/web-hsin-07-08-04.asp].

[18] U.S. Department of Homeland Security, "Homeland Security Information Network to Expand Collaboration, Connectivity for States and Major Cities," available at [http://www.dhs.gov/dhspublic/display?content=3350].

[19] Justin Rood, "Pentagon Has Access to Local Police Intelligence Through Office in Homeland Security Department," *CQ Homeland Security*, July 6, 2004, available at [http://www.cq.com/corp/show.do?page=temp/20040708_homeland].

[20] Brian Robinson, "DHS Unfolds New Safety Net," *Federal Computer Week*, June 21, 2004, available at [http://www.fcw.com/supplements/homeland/2004/sup2/hom-safety-06-21-04.asp].

information, although DHS plans to upgrade the security of the network to allow for the exchange of security classified information at the "Secret" level by fall 2004. These information protections are discussed later in this report. In the future, DHS also plans to develop an interface between JRIES and RISSNET (see below), a long-established nationwide network of criminal databases used by law enforcement agencies.[21]

Regional Information Sharing System (RISS) Program. The RISS Program is an established system of six regional centers that are used to "share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines."[22] The RISS Program was created to combat traditional law enforcement targets, such as drug trafficking and violent crime, but has been expanded to include other activities, such as terrorism and cybercrime. According to its website, RISS has "member agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England."[23] The RISS program uses a regional approach, so that each center can tailor/focus its resources on the specific needs of its area, while still coordinating and sharing information as one body for national-scope issues.[24]

The origins of the RISS Program date to 1974, when the Department of Justice awarded its first grant to allow police departments in the southern U.S. to share/exchange information with each other via computers.[25] This support helped create the first of the six regional centers, the Regional Organized Crime Information Center (ROCIC).[26] The other regional centers include the Rocky Mountain Information Network (RMIN),[27] the New England State Police Information Network (NESPIN),[28] the Mid-States Organized Crime Information Center (MOCIC),[29] the

---

[21] U.S. Department of Homeland Security, "Homeland Security Information Network to Expand Collaboration, Connectivity for States and Major Cities," available at [http://www.dhs.gov/dhspublic/display?content=3350].

[22] For a detailed description of RISS, see [http://www.iir.com/riss/] and [http://www.rissinfo.com/].

[23] See [http://www.rissinfo.com/overview2.htm].

[24] See [http://www.rissinfo.com/].

[25] Wilson P. Dizard III, "IT Security Calls for Collaboration," *Government Computer News*, Mar. 4, 2002, available at [http://www.gcn.com/21_5/news/18099-1.html]; U.S. Department of Justice, Bureau of Justice Assistance, "Regional Information Sharing Program," *Bureau of Justice Assistance Program Brief* (Washington: April 2002), available at [http://www.ncjrs.org/pdffiles1/bja/192666.pdf].

[26] Regional member states include Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, and West Virginia. Puerto Rico and the U.S. Virgin Islands are also members of ROCIC.

[27] Regional member states include Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming. RMIN also includes member agencies from Canada.

[28] Regional member states include Connecticut, Maine, Massachusetts, New Hampshire, (continued...)

Western States Information Network (WSIN),[30] and the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN).[31] Membership in each of the centers includes federal, state, and local law enforcement agencies, for an estimated total of "nearly 7,000 law enforcement and criminal justice agencies representing over 700,000 sworn officers."[32] The RISS Program continues to be federally funded through the Bureau of Justice Assistance (BJA) at the Department of Justice (DOJ), which also has program management oversight responsibilities. In addition, RISS centers are required to be in compliance with Criminal Intelligence Systems Operating Policies regarding the confidentiality of information collected and shared.[33] Each RISS center provides its member agencies with a range of services, including:

- **Information sharing** — primarily through the operation of the RISS secure intranet (RISSNET) (see below), providing secure databases and investigative tools.

- **Analysis** — including the preparation of analytical products, compilation and analysis of data, and computer forensics analysis.

- **Equipment loans** — inventories of specialized investigative and surveillance equipment, including photographic, communications, and surveillance equipment, for member agencies to borrow for multijurisdictional investigations.

- **Confidential funds** — following federal and center guidelines, money that can be used to purchase information, contraband, stolen property, and other evidentiary items, as well as to pay investigative expenses for multijurisdictional investigations.

- **Training** — meetings and conferences for training on information sharing techniques, anti-terrorism training; and training in

---

[28] (...continued)
Rhode Island, and Vermont. NESPIN also includes member agencies from Canada.

[29] Regional member states include Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin. MOCIC also includes member agencies from Canada.

[30] Regional members states include Alaska, California, Hawaii, Oregon, and Washington. WSIN also includes member agencies from Canada, Australia, and Guam.

[31] Regional members states include Delaware, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, and Pennsylvania, as well as the District of Columbia. MAGLOCLEN also includes member agencies from England, the Canadian provinces of Ontario and Quebec, and Australia.

[32] See [http://www.rissinfo.com/overview2.htm].

[33] See 28 C.F.R. Part 23; U.S. Department of Justice, Bureau of Justice Assistance, "The RISS Program: 2002, Membership and Service Activity"(Washington: June 2003), available at [http://www.iir.com/Publications/RissProgram2002.pdf].

surveillance techniques, equipment use, safety, and analysis techniques.

- **Technical assistance** — training and assistance for activities such as requesting analytical services, and RISSNET installation and support.[34]

The centerpiece of the RISS Program's information sharing activities is its secure intranet, RISSNET, which is capable of sharing electronically what is termed "sensitive but unclassified information." RISSNET participants can either connect a single computer to the intranet, or establish a node connection, enabling wider access through their agency's network. RISSNET participants use a virtual private network (VPN) connection over the Internet to access the RISSNET gateway firewall, whereupon the user's identity is authenticated and access is granted to the secure intranet. The secure intranet is a dedicated network carried over frame relay circuits (a guaranteed amount of bandwidth carried over public telephone lines) connecting the RISS centers to the database resources. Security is maintained through the use of encryption, smart cards, and other Internet security protocols.[35] This system enables participants to send and receive secure e-mail transmissions with other RISSNET participants, as well as use secure Web browser sessions to access data. RISSNET also provides access to a number of other resources, including:

- **RISS center websites** — each of the six RISS centers has a website that provides information on its services and resources, and provides access to criminal intelligence databases.

- **RISSIntel/RISSNET II** — electronically linked collection of web-based criminal intelligence databases with information provided by member agencies.

- **RISSGang** — the RISS National Gang Database, a crime-specific database related to gangs and gang members, including both text information and images, such as photographs, gang tattoos, and gang graffiti.

- **RISSLeads** — the RISS Investigative Leads Bulletin Board, a newsgroup server where participants can post case-related information for the purpose of generating investigative leads and can exchange information with other participants.

---

[34] See [http://www.rissinfo.com/services.htm].

[35] U.S. Department of Justice, Bureau of Justice Assistance, "The RISS Program: 2002, Membership and Service Activity," available at [http://www.iir.com/Publications/RissProgram2002.pdf]; Office of Information Technology, Regional Information Sharing Systems, "Regional Information Sharing — What's Working? Is It Helping?," July 21, 2003, National Criminal Justice Association National Forum 2003 Conference, available at [http://www.ijis.org/education/Docs/RISS/RISS%20Tech%20(RISS).ppt].

- **RISSSearch** — a search engine that identifies and retrieves data from multiple databases and information sources, including restricted information sites, sensitive but unclassified sites, and public Internet sites.

- **RISSTraining** — electronic resources for anti-terrorism training.

- **RISSLinks** — a data visualization tool for analyzing and showing associations among the results from multiple databases.

- **RISSLive** — an online, real-time communications medium to facilitate real-time information sharing among participants.[36]

Another recently developed resource is the RISS Anti-Terrorism Information Exchange (ATIX). Initiated in late 2002, RISS ATIX represents an expansion of the efforts to facilitate communication and information sharing among personnel responsible for planning and implementing actions to prevent, mitigate, and recover from terrorist incidents and disasters. RISS ATIX participants include constituencies that have not traditionally participated in RISS. RISS ATIX participants include both government and private sector actors, who are divided into ATIX communities, based on their functions.[37] According to the RISS ATIX website, some of the ATIX communities include "state, county, local, tribal, and federal government; law enforcement; emergency management; disaster relief; utilities; and, among others, the chemical, transportation, and telecommunication industries."[38] Since becoming operational, RISS ATIX has been used to facilitate communications for events such as Hurricane Isabel in September 2003, the G8 Summit at Sea Island, Georgia, in June 2004, and both the Republican and Democratic national conventions in summer 2004.[39]

RISS ATIX utilizes four primary components to facilitate communication and information sharing. These include:

---

[36] U.S. Department of Justice, Bureau of Justice Assistance, "The RISS Program: 2002, Membership and Service Activity," available at [http://www.iir.com/Publications/RissProgram2002.pdf]; National Narcotic Officers' Associations' Coalition, "Regional Information Sharing Systems Program," *NNOAC Insight*, n.d., available at [http://www.natlnarc.org/papers/RISS_Position.pdf]; Gerard P. Lynch, "Facilitating an Enhanced Information Sharing Network That Links Law Enforcement and Homeland Security for Federal, State, and Local Governments," hearing statement before U.S. Congress, House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Affairs, and the Census (Washington: July 13, 2004).

[37] U.S. Department of Justice, Bureau of Justice Assistance, "The RISS Program: 2002, Membership and Service Activity," available at [http://www.iir.com/Publications/RissProgram2002.pdf].

[38] See [http://www.rissinfo.com/rissatix.htm].

[39] Lynch, "Facilitating an Enhanced Information Sharing Network that Links Law Enforcement and Homeland Security for Federal, State, and Local Governments," hearing statement.

- **RISS ATIX Web page** — news articles, online resources, and contact information tailored to the various ATIX communities.

- **RISS ATIX bulletin board** — a newsgroup server where participants can post information related to terrorism, disasters, and homeland security, as well as "page" online participants and send secure e-mail messages.

- **ATIXLive** — an online, real-time communications medium to facilitate real-time information sharing among participants, including the "paging" function and the ability to send secure e-mail messages from within the ATIXLive application.

- **ATIX secure e-mail** — a secure e-mail application to send and receive homeland security alerts and exchange information with other participants.[40]

On September 1, 2002, RISSNET interconnected with the FBI Law Enforcement Online (LEO) system to create a so-called "virtual single system" for the purpose of exchanging sensitive but unclassified homeland security information. Both RISSNET and LEO participants can access these resources combined using a single logon identifier. Participants can also exchange secure e-mail messages. RISSNET has established, or is in the process of establishing, interconnections with other information sharing networks as well, including the National Law Enforcement Telecommunications System (NLETS), the Criminal Information Sharing Alliance (CISAnet), and the Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Project.[41] As with other information sharing initiatives, civil liberties organizations have raised concerns about privacy and the potential misuse of personal data as more information sources become interconnected and available to a larger number of users.

Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Information Sharing Project. The MATRIX project was initially developed in the days following the September 11, 2001, terrorist attacks by Seisint, a Florida-based information products company, in an effort to facilitate collaborative information sharing and factual data analysis. At the outset of the project, MATRIX included a component Seisint called the High Terrorist Factor (HTF), which was designed to identify individuals with high HTF scores, or so-called terrorism quotients, based on an analysis of demographic and behavioral data. Although the HTF scoring system appeared to attract the interest of officials, this feature was

---

[40] See [http://www.rissinfo.com/rissatix.htm].

[41] U.S. Department of Justice, Bureau of Justice Assistance, "The RISS Program: 2002, Membership and Service Activity," available at [http://www.iir.com/Publications/RissProgram2002.pdf]; National Narcotic Officers' Associations' Coalition, "Regional Information Sharing Systems Program," available at [http://www.natlnarc.org/papers/RISS_Position.pdf]; Lynch, "Facilitating an Enhanced Information Sharing Network That Links Law Enforcement and Homeland Security for Federal, State, and Local Governments," hearing statement.

reportedly dropped from MATRIX because it relied on intelligence data not normally available to the law enforcement community and because of concerns about privacy abuses.[42]

In its current form, the MATRIX pilot project is administered through a collaborative effort between Seisint, the Florida Department of Law Enforcement (FDLE),[43] and the Institute for Intergovernmental Research (IIR), a "Florida-based nonprofit research and training organization, [that] specializes in law enforcement, juvenile justice, and criminal justice issues."[44] FDLE serves as the "security agent" for MATRIX, administering control over which agencies and individuals have access to the system. FDLE is also a participant state in MATRIX. IIR is responsible for administrative support, and is the grantee for federal funds received for MATRIX.[45] Thus far, it has been reported that the MATRIX pilot project has received a total of $12 million in federal funding — $8 million from the Office of Domestic Preparedness (ODP) at the Department of Homeland Security (DHS), and $4 million from the Bureau of Justice Assistance (BJA) at the Department of Justice (DOJ).[46]

The analytical core of the MATRIX pilot project is an application called Factual Analysis Criminal Threat Solution (FACTS), described as a "technological, investigative tool allowing query-based searches of available state and public records in the data reference repository."[47] The FACTS application allows an authorized user to search "dynamically combined records from disparate datasets" based on partial information, and will "assemble" the results.[48] The data reference repository used with FACTS represents the amalgamation of over 3.9 billion public records collected from thousands of sources.[49] The data contained in FACTS include FAA pilot license and aircraft ownership records, property ownership records, information on vessels registered with the Coast Guard, state sexual offender lists, federal terrorist watch lists, corporation filings, Uniform Commercial Code filings, bankruptcy filings, state-issued professional license records, criminal history information, department of corrections information and photo images, driver's license information and photo images, motor vehicle registration information, and information from

---

[42] Brian Bergstein, "Database Firm Tagged 120,000 Terrorism 'Suspects' for Feds," (Biloxi, MS) *SunHerald*, May 20, 2004, available at [http://www.sunherald.com/mld/sunherald/business/technology/8715327.htm].

[43] The FDLE website is available at [http://www.fdle.state.fl.us/].

[44] The IIR website is available at [http://www.iir.com/].

[45] See [http://www.matrix-at.org/roles.htm].

[46] John Schwartz, "Privacy Fears Erode Support for a Network to Fight Crime," *New York Times*, Mar. 15, 2004, available at [http://www.nytimes.com/2004/03/15/technology/15matrix.html]; see also [http://www.matrix-at.org/faq.htm].

[47] For a more detailed description of FACTS, see [http://www.matrix-at.org/FACTS_defined.htm].

[48] Ibid.

[49] See [http://www.matrix-at.org/newsletter.pdf].

commercial sources that "are generally available to the public or legally permissible under federal law."[50]

The data reference repository is said to exclude data such as telemarketing call lists; direct mail mailing lists; airline reservations or travel records, frequent flyer/hotel stay program membership information or activity; magazine subscription records; information about purchases made at retailers or over the Internet; telephone calling logs or records; credit or debit card numbers; mortgage or car payment information; bank account numbers or balance information; records of birth certificates, marriage licenses, and divorce decrees; and utility bill payment information. Participating law enforcement agencies utilize this information sharing and data mining resource over the Regional Information Sharing Systems (RISS) secure intranet (RISSNET), described above.

Some civil liberties organizations have raised concerns about law enforcement actions being taken based on algorithms and analytical criteria developed by a private corporation — in this case, Seisint — without any public or legislative input.[51] Questions have also been raised about the level of involvement of the federal government, particularly the Department of Homeland Security and the Department of Justice, in a project that is ostensibly focused on supporting state-based information sharing.[52]

The MATRIX pilot project has suffered some setbacks in recruiting states to participate. The lack of participation can be especially troubling for a networked information sharing project such as MATRIX because, as Metcalfe's Law suggests, "the power of the network increases exponentially by the number of computers connected to it."[53] While as many as 16 states have been reported to have either participated or seriously considered participating in MATRIX at its outset, several have chosen to withdraw, leaving a current total of five states, including Florida, Michigan, Ohio, Pennsylvania, and Connecticut, actively participating. State officials have cited a variety of reasons for not participating in MATRIX, including costs, concerns about violating state privacy laws, and duplication of existing resources.[54]

---

[50] For more information about data included in and excluded from the data reference repository, see [http://www.matrix-at.org/data_sources.htm].

[51] William Welsh, "Feds Offer to Mend Matrix," *Washington Technology*, May 24, 2004, available at [http://www.washingtontechnology.com/news/19_4/egov/23597-1.html].

[52] Robert O'Harrow, Jr., "Anti-Terror Database Got Show at White House," *Washington Post*, May 21, 2004, p. A12.

[53] For a more detailed discussion of Metcalfe's Law, see [http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214115,00.html].

[54] The states that have reportedly decided to withdraw from the pilot project include Alabama, California, Georgia, Kentucky, Louisiana, New York, Oregon, South Carolina, Texas, Utah, and Wisconsin. Larry Greenemeier, "Two More States Withdraw from Database," *InformationWeek*, Mar. 12, 2004, available at [http://www.informationweek.com/story/showArticle.jhtml?articleID=18312112]; Diane Frank, "Utah No Longer Part of

(continued...)

To help address the privacy concerns associated with a centralized data repository, some officials have suggested switching to a distributed approach whereby each state would maintain possession of its data and control access according to its individual laws. As a pilot project, MATRIX is expected to continue through November 2004. At that time, IIR will submit a final report to officials evaluating the long-term viability of the project.[55]

Projected Arrangements

At this time it is unclear if and how the 9/11 Commission report recommendations regarding information sharing might be implemented. One option would be to use and/or modify existing information sharing initiatives, including the possibility of combining features from existing initiatives. Another option might be to build a new information sharing infrastructure from the ground up. However, in light of the level of resources already invested in existing information sharing initiatives, the cost and time involved to build a new infrastructure, and the urgency that some place on implementing some of the recommendations quickly, it appears that a comprehensive information sharing initiative would most likely involve capitalizing on existing resources and working to improve the interoperability of these resources.

As described above, some information sharing networks already exist, although they each have their own specific purposes and goals. One option might be to construct a network of networks that incorporates existing information sharing networks and other databases and resources that could create the trusted information network called for in the 9/11 Commission report. In keeping with the recommendation of the second report of the Markle Foundation's Task Force on National Security in the Information Age, which was cited by the 9/11 Commission report, such a network would not utilize either a mainframe or a hub-and-spoke model of information dissemination, both of which feature centralized points for information flows.[56] Instead, the trusted information network could operate as a decentralized peer-to-peer network. This approach would allow participants to retain control over their respective data, while also reducing the vulnerability of the information sharing network to attack or failure by not having a single control point or hub upon which the rest of the system would be dependent. Through the use of middleware — software used to connect or integrate two or more separate

---

[54] (...continued)
MATRIX," *Federal Computer Week*, Apr. 5, 2004, p. 14; Associated Press. "Two More States Withdraw from Controversial Database Program," (Fort Worth-Dallas, TX) *Star-Telegram*, Mar. 12, 2004, available at [http://www.dfw.com/mld/dfw/business/8170978.htm?1c]; Associated Press "Matrix Plan Fuels Privacy Fears," *Wired News*, Feb. 2, 2004, available at [http://www.wired.com/news/business/0,1367,62141,00.html].

[55] Welsh, "Feds Offer to Mend Matrix," available at [http://www.washingtontechnology.com/news/19_4/egov/23597-1.html].

[56] See the "Overview" in Markle Foundation, Task Force on National Security in the Information Age, *Creating a Trusted Information Network for Homeland Security: Second Report of the Markle Foundation Task Force* (New York: December 2003), n.p., available at [http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf].

applications — the challenges of making diverse databases interoperable, or compatible, might be addressed. Middleware could also be designed to support a rule-based system that could govern which data could be accessed, who could access the data, and how the data could be used. A rule-based system could incorporate the overarching policy framework recommended by the 9/11 Commission report, as well as jurisdiction-specific privacy and security requirements.

In light of the emphasis being placed on information sharing, and the complexity of the issue, it is likely that the creation of a trusted information network is likely to require the dedicated attention of key individuals over an extended period of time. From a technology management perspective, a chief information sharing officer could be designated within OMB, as well as at each of the relevant agencies. These individuals could serve as the primary points of contact for information sharing initiatives, and could be responsible for working with their respective chief information officers and agency managers to facilitate compliance with standard setting and information sharing requirements. The institutionalization of a chief information sharing position to champion information sharing might also help ensure that agencies do not eventually revert to their previous practices.

Related Policy

The development of information sharing for homeland security purposes, as the above discussion of some of the existing arrangements suggests, occurs within an existing policy context, which may prove to be in need of clarification, adjustment, and supplement. For example, state privacy laws, as noted, apparently have limited participation in the MATRIX pilot project. Some federal policy considerations that bear on information sharing are discussed in this section relative to anticipated presidential procedures mandated by the Homeland Security Act.

Presidential Procedures. Signed into law on November 25, 2002, the Homeland Security Act, establishing the principal homeland security institutions of the federal government, contains various provisions facilitating or mandating homeland security information sharing. Primary among these is Section 892 of the statute, which defines "homeland security information" as "any information possessed by a Federal, State, or local agency that (A) relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; and (D) would improve the response to a terrorist act."[57]

Prior to this definition of homeland security information, five subsections establish procedures and conditions regarding such information. The first of these requires the President to

> prescribe and implement procedures under which relevant Federal agencies (A) share relevant and appropriate homeland security information with other Federal agencies, including the Department [of Homeland Security] and appropriate State and local personnel; (B) identify and safeguard homeland security information

---

[57] 116 Stat. 2255.

> that is *sensitive but unclassified*; and (C) to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information [from its protected status], as appropriate, and with which such personnel it may be shared after such information is removed.[58]

Neither this section nor the other provisions of the Homeland Security Act define what constitutes "sensitive but unclassified" homeland security information. The remaining portions of the subsection require the President to "ensure that such procedures [as he prescribes] apply to all agencies of the Federal Government"; stipulate that these new procedures "shall not change the substantive requirements for the classification and safeguarding of classified information"; and specify that the new procedures "shall not change the requirements and authorities to protect [intelligence] sources and methods."

The second subsection prescribes refinements to the procedures established by the President pursuant to the first subsection. "Under [the] procedures prescribed by the President," it is stated, "all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with" the President's procedures, "together with assessments of the credibility of such information." Each of these information sharing systems must

> (A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ; (B) have the capacity to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know such information; (C) be configured to allow the efficient and effective sharing of information; and (D) be accessible to appropriate State and local personnel.

Other provisions require the establishment of conditions on the use of shared information "(A) to limit the redissemination of such information to ensure that such information is not used for an unauthorized purpose; (B) to ensure the security and confidentiality of such information; (C) to protect the constitutional and statutory right of any individuals who are subjects of such information; and (D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information." The information sharing systems are to "include existing information sharing systems, including, but not limited to, the National Law Enforcement Telecommunications System, the Regional Information Sharing System, and the Terrorist Threat Warning System of the Federal Bureau of Investigation ." Federal agencies having access to information sharing systems have access to all of the information shared in those systems. The prescribed procedures are to "ensure that appropriate State and local personnel are authorized to use such information sharing systems (A) to access information shared with such personnel; and (B) to share, with others who have access to such information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity." Regarding this shared state

---

[58] 116 Stat. 2253 (emphasis added).

and local information, it is to be reviewed and assessed, under procedures prescribed jointly by the Director of Central Intelligence (DCI) and the Attorney General, by each appropriate federal agency, as determined by the President, and integrated with existing intelligence.[59]

The third subsection authorizes the President to "prescribe procedures under which Federal agencies may, to the extent the President considers necessary, share with appropriate State and local personnel homeland security information that remains classified or otherwise protected" after being reviewed for removal from its protected status. To facilitate such sharing, a sense of Congress provision recognizes the use of background investigations and security clearances, non-disclosure agreements regarding sensitive but unclassified information, and "information-sharing partnerships that include appropriate State and local personnel, such as the Joint Terrorism Task Forces of the Federal Bureau of Investigation, the Anti-Terrorism Task Forces of the Department of Justice, and regional Terrorism Early Warning Groups."

The fourth subsection specifies that the head of each affected agency shall designate an official having administrative responsibility for that agency's compliance with the information sharing requirements of Sections 891-899.[60]

Finally, the fifth subsection states: "Under procedures prescribed under this section, information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information." Presumably, it is the President who prescribes the referred to procedures; information shared with a subnational jurisdiction pursuant to these procedures remains under the "control" of the providing federal agency; and, because the information is under federal "control," it is beyond the scope of state information access or freedom of information laws.

On July 29, 2003, President Bush issued E.O. 13311, assigning responsibility for preparing the Section 892 homeland security information sharing procedures to the Secretary of Homeland Security.[61] Others, in accordance with the provisions of the order, will make input, as well, including the Attorney General, the DCI, and specified officials with whom Homeland Security Secretary Ridge is to coordinate. How that set of procedures will be formulated has not been made publicly known by the Department of Homeland Security (DHS). While many observers expected that these procedures would be issued during the summer of 2004, they have not appeared to date.

Control. Arising with the formulation of the President's procedures is the important consideration of the "ownership" or control of shared information. For the

---

[59] 116 Stat. 2254.

[60] These provisions constitute Subtitle I of Title VIII of the Homeland Security Act and may be cited, as specified in the statute, as the Homeland Security Information Sharing Act.

[61] *Federal Register*, vol. 68, July 31, 2003, pp. 45149-45150.

information sharing procedures mandated by Section 892 of the Homeland Security Act, Congress has determined in Subsection 892(e) that "information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency." The subsection further specifies that such shared federal agency information is not subject to "a State or local law authorizing or requiring such a government to disclose information."

The statute is silent regarding any reciprocal "controls" which state or local governments may exercise regarding information they provide through the sharing system. Whether such information as state or local governments do provide would constitute, as a threshold question, a federal "agency record" accessible under the Freedom of Information Act (FOIA) is not immediately clear. The Supreme Court, because the FOIA provides no definition of an "agency record," established, several years ago, in *DOJ* v. *Tax Analysts*, a two-prong test for determining whether materials so qualify. First, a federal agency must "either create or obtain" the materials, and, second, "must be in control of the requested materials at the time the FOIA request is made," control meaning "that the materials have come into the agency's possession in the legitimate conduct of its official duties."[62] Would federal agencies be considered to have "obtained" state or local government information voluntarily provided through the sharing system? Does the voluntary provision of such information through the sharing system result in its coming under federal agency "control," that is "the agency's possession in the legitimate conduct of its official duties?"

It seems likely that, if a court is asked to determine whether state or local government information voluntarily provided through the sharing system falls within the scope of the FOIA, it would examine the extent to which a federal agency or agencies had control over the materials at issue. Beyond this threshold question, should a court consider whether such information is subject to FOIA, it is a matter of the applicability of the statute's nine exemptions to the rule of disclosure and other provisions protecting law enforcement information.[63]

Protections. The President's procedures for sharing homeland security information must accommodate various kinds of protected information. Section 892(a) of the Homeland Security Act requires the President to "identify and safeguard homeland security information that is sensitive but unclassified; and ... to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed." Moreover, the new procedures "shall not change the substantive requirements for the classification and safeguarding of classified information" and "shall not change the requirements and authorities to protect [intelligence] sources and methods." Following Subsection 892(a), the President is directed, when prescribing the mandated information sharing procedures, "to protect the constitutional and statutory rights of any individuals who

---

[62] *DOJ* v. *Tax Analysts*, 492 U.S. 136, 144-145 (1989).

[63] See 5 U.S.C. § 552(b)-(c).

are subjects of such information."[64] Among the types of protected information so identified are those which are "sensitive but unclassified," those which are classified, and those which may enjoy privacy protection, as well as intelligence sources and methods.

There is a degree of uncertainty about the meaning and scope of some of these terms, however, and management requirements for a couple of types of protected information proffer compliance difficulties for subnational governments. As mentioned earlier, neither Section 892 nor the other provisions of the Homeland Security Act define what constitutes "sensitive but unclassified" homeland security information. Some have noted that the Computer Security Act of 1987 refers to, and defines, "sensitive information," but neither this statute nor its definition of "sensitive information" is referenced by the Homeland Security Act regarding "sensitive but unclassified" information.[65] Furthermore, the Computer Security Act, as originally enacted, specified that it was not to be construed to constitute authority to withhold information sought pursuant to the FOIA or to authorize any federal agency to limit, restrict, regulate, or control, among other actions, the disclosure, use, transfer, or sale of any information disclosable under the FOIA or public domain information.[66]

Elsewhere, in Section 208 of the E-Government Act of 2002, allowance is made for the modification or waiver of a required privacy impact assessment "for security reasons, or to protect classified, sensitive, or private information contained in an assessment."[67] What constitutes "sensitive" information for this section is not evident, because the term is neither defined in the statute nor is its relationship, if any, to the "sensitive but unclassified" information of Section 892 of the Homeland Security Act explained.

An internal DHS management directive on "Safeguarding Sensitive But Unclassified (For Official Use Only) Information," issued on May 11, 2004, indicates that the "For Official Use Only" (FOUO) marking "will be used to identify sensitive but unclassified information within the DHS community that is not otherwise specifically described and governed by statute or regulation." Examples of several types of information treated as FOUO information are provided, such as information that may be protectable under the FOIA's exemptions to the rule of disclosure; international and domestic information protected by statute, treaty, or other agreements; "[i]nformation that could be sold for profit"; "[i]nformation that could result in physical risk to personnel"; and information revealing security vulnerabilities or breaching operations security. Access to FOUO information is on a need-to-know basis, and persons having such access must sign a nondisclosure agreement. Secure storage of FOUO information is required, and secure communication of it by encrypted telephone or fax is encouraged.[68]

---

[64] 116 Stat. 2253-2254.

[65] See 101 Stat. 1724; 15 U.S.C. § 278g-3.

[66] 101 Stat. 1730; 40 U.S.C. § 759 note, subsequently repealed 1996, 110 Stat. 680.

[67] 116 Stat. 2922.

[68] U.S. Department of Homeland Security, Management Directive System, "Safeguarding (continued...)

While statutorily undefined, the "sensitive but unclassified" homeland security information concept perhaps may be discerned in a practice disclosed in regard to the operations of a new facility, a $4 million expansion of the Upstate New York Regional Intelligence Center, jointly operated by New York State and the FBI. Managers explained that security classified information, including data about individuals, would be "filtered" through screeners and intelligence analysts at the center so that no classified information would be provided to local authorities. Thus, it appeared that details which merited security classification would be eliminated or obscured, resulting in unclassified information which would still not be available to the public.[69] This unclassified information will probably be regarded as having been compiled for law enforcement purposes and, as such, protected from disclosure under the FOIA or comparable New York law. It seems unlikely, however, that "sensitive but unclassified" homeland security information, per se, could be protected from disclosure pursuant to the FOIA because it does not appear to fall clearly within any of that statute's exemptions.

Classified information is understood to be information "specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy," and which is "in fact properly classified pursuant to such Executive order."[70] The operative executive order prescribing security classification (and declassification) policy and practice is E.O. 12958 of April 17, 1995, as amended by E.O. 13292 of March 25, 2003.[71] The latter directive added two new concerns to the former's rather traditional, but specific, military, intelligence, foreign affairs, and national security classification categories: defense against transnational terrorism and the vulnerabilities of infrastructures, both of which are probably regarded generally to be homeland security interests. Security classification is used to protect Restricted Data, as defined by the Atomic Energy Act of 1954, and intelligence sources and methods, the sanctity of which is a statutorily specified responsibility of the DCI.[72] Other types of information protected by security classification include National Security Agency signals intelligence and communications security information, and so-called foreign government information, which is information provided by a foreign government or international organization of governments, with the expectation that the information, its source, or both, are to be held in confidence.

Two types of privileged homeland security information not regarded to be security classified information, but which may be considered to be "sensitive but unclassified," although the DHS management directive on FOUO information suggests otherwise, are "critical infrastructure information," as understood within the

---

[68] (...continued)
Sensitive But Unclassified (For Official Use Only) Information," MD No. 11042, May 11, 2004.

[69] David Johnston, "Terror Data to Be Shared at New Center Near Albany," *New York Times*, May 25, 2004, p. A20.

[70] 5 U.S.C. § 551(b)(1).

[71] 3 C.F.R., 1995 Comp., pp. 333-356; 3 C.F.R., 2003 Comp., pp. 196-218.

[72] See 42 U.S.C. § 2014(y); 50 U.S.C. § 403-3(c)(6).

context of Subtitle B of Title II of the Homeland Security Act, and "Sensitive Security Information" (SSI), as that term is defined by the Transportation Security Administration. In defining "critical infrastructure information" in Subtitle B of Title II of the Homeland Security Act, the statute recognizes that this information is "not customarily in the public domain." When voluntarily shared with DHS by the private sector, it becomes subject to certain protections, including exemption from disclosure under the FOIA and specified use limitations (sharing with state or local governments is anticipated). Federal officers or employees improperly disclosing such critical infrastructure information may be criminally punished.[73] Operative security classification policy does not authorize the classification of this information, which remains the private property of the submitter.[74]

Relying upon information protection provisions of the Air Transportation Security Act of 1974 and the Aviation and Transportation Security Act of 2001, the Transportation Security Administration, now a component of DHS, has issued transportation security regulations making reference to "Sensitive Security Information" (SSI), defined as "information about security programs, vulnerability assessments, technical specifications of certain screening equipment and objects used to test screening equipment, and other information."[75] A more detailed explanation of SSI may be found in the regulations.[76] While SSI is a type of protected information, it is not security classified, but may constitute "sensitive but unclassified" homeland security information. A federal appellate court ruled in 1993 that 1990 amendments did not by implication repeal the authority of the Air Transportation Security Act of 1974 to promulgate and withhold from the public security-sensitive rules and other related information now within the scope of SSI.[77]

Speaking at the summer meeting of the National Governors Association in 2003, Secretary Ridge indicated that, in addition to the governors, five senior officials in each state would be given a Top Secret security clearance in order that security classified information might be shared with them for homeland security purposes.[78] Presumably, the states paid for the background investigations for these clearances,

---

[73] See 116 Stat. 2150-2155.

[74] The Fifth Amendment to the Constitution, among other prohibitions, specifies that no person shall "be deprived of life, liberty, or property, without due process of law." Pursuant to the Invention Secrecy Act, however, the federal government may deny, for one year, subject to renewal, the issuance of a patent to an applicant where the publication of the application or granting of the patent would be "detrimental to the national security." An inventor who violates the imposed requirement to keep his invention secret may be criminally punished and regarded to have forfeited patenting his invention. See 35 U.S.C. § 181-188; see, also, 50 U.S.C. App. 10((i).

[75] See 49 U.S.C. § 114(s), 40119; this general definition of SSI appears in *Federal Register*, vol. 67, Feb. 22, 2002, p. 8342.

[76] See 49 C.F.R. 1520.7.

[77] See *Public Citizen, Inc.* v. *FAA*, 988 F.2d 186 (D.C. Cir. 1993).

[78] Michael Janofsky, "Intelligence to Be Shared, Ridge Tells Governors," *New York Times*, Aug. 19, 2003, p. A17; the prepared text of Secretary Ridge's remarks is available at [http://www.dhs.gov/dhspublic/display?theme=44&content=1200&print=true].

each costing upwards of $2,500, and perhaps used discretionary federal homeland security grant funds for this expense. Whether this number of clearances is adequate for each state, given population, geography, and other differences, is uncertain. How these state officials will be able to use classified information to direct the actions of other uncleared state personnel is somewhat problematic, as are integrity considerations of detecting and addressing security breaches involving classified information.

Quality. Finally, for policymakers, Section 892 seems to require some attention to data quality in the homeland security information sharing procedures to be prescribed by the President. Shared information is to be provided "together with assessments of the credibility of such information." Presumably, these assessments would be made by the information provider. Potentially more controversial is the requirement that shared state and local information "be reviewed and assessed, under procedures prescribed jointly by the Director of Central Intelligence and the Attorney General, by each appropriate Federal agency, as determined by the President, and integrated with existing intelligence." The nature of this assessment is left to determination by the named principals. The section would also have the President's information sharing procedures "provide data integrity through the timely removal and destruction of obsolete or erroneous names and information," a rather broad and highly discretionary standard. Who would function as the shared information system manager regarding this data integrity responsibility is not clear, nor is the extent to which other federal records management law, such as Chapters 31 and 33 of Title 44, United States Code, is applicable.

GAO Evaluations

In September 2003 testimony before two subcommittees of the House Select Committee on Homeland Security, Robert F. Dacey, Director of Information Security Issues for GAO, discussed, among other information sharing matters, the federal government's critical information protection (CIP) effort, "which is focused on the sharing of information on incidents, threats, and vulnerabilities, and the providing of warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments and the private sector." Acknowledging that "improvements have been made," further efforts were thought to be needed to address the following critical CIP challenges:

- developing a comprehensive and coordinated national plan to facilitate CIP information sharing that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;

- developing fully productive information sharing relationships within the federal government and between the federal government and state and local governments and the private sector;

- improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate, timely, useful warnings and other

information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector; and

- providing appropriate incentives for nonfederal entities to increase information sharing with the federal government and enhance other CIP efforts.[79]

Recounting various recent CIP developments, Dacey noted the 1998 issuance of Presidential Decision Directive 63, which "established CIP as a national goal and described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government," as well as "organizations to provide central coordination and support." Critical infrastructure sectors essential to national security, national economic security, and/or national public health and safety were identified. "For these sectors, which now total 14, federal government leads (sector liaisons) and private-sector leads (sector coordinators) were to work with each other to address problems related to CIP for their sector" through the development and implementation of vulnerability and education programs and a sectoral preparation plan assessing sector vulnerabilities to cyber or physical attack, as well as ways to eliminate significant vulnerabilities, and identify, prevent, respond to, and recover from attacks. The "voluntary creation of information sharing and analysis centers (ISACs) to serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government" was encouraged. Dacey identified 15 established ISACs and a prospective center in the maritime transportation sector.[80]

"An underlying issue in the implementation of CIP," according to the GAO testimony, "is that no national plan to facilitate information sharing yet exists that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets time frames for achieving objectives, and establishes performance measures." Such a plan, which GAO, since 1998, has called for and "made numerous related recommendations regarding," would appear to be outside of the scope of the homeland security information sharing procedures mandated by Section 892 of the Homeland Security Act (although the creation of the procedures seemingly would benefit from having such a plan). The plan is, however, anticipated in the *National Strategy for Homeland Security*, which indicates that its creation will build on "baseline physical and cyber infrastructure protection plans" then under development and subsequently produced in February 2003 as the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* and the *National Strategy to Secure Cyberspace*.[81] The President's November 2002 DHS reorganization plan tasks the department's Assistant Secretary for Infrastructure Protection with developing "a national plan for securing the key resources and critical

---

[79] U.S. General Accounting Office, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO Testimony GAO-03-1165T (Washington: Sept. 17, 2003), pp. 2-3.

[80] Ibid., pp. 12-15.

[81] See U.S. Office of Homeland Security, *National Strategy for Homeland Security* (Washington: July 2002), p. 33.

infrastructure of the United States," and specifies certain systems to be included in such a plan.[82]

Six months later, in a reprise, Dacey appeared before the same subcommittees of the House Select Committee on Homeland Security to discuss the status of ISACs. Operative CIP policy "left the actual design and function of the ISACs to the entities that formed them," he explained. "As a result, although their overall missions are similar, the current ISACs were established and developed based on the unique characteristics and needs of their individual sectors. They operate under different management and operational structures," he continued, "and, among other things, have different business models and funding mechanisms." While "most are managed or operated as private entities," some "are part of associations that represent their sectors" and others "have partnered with government agencies." The "funding mechanisms used by the ISACs include fee-for-service, association sponsorship, federal grants, and/or voluntary or in-kind operations by ISAC participants."[83]

Dacey proffered examples of the various methods being used by ISACs to share information with their members, other ISACs, and the federal government. These methods include:

- Member access to electronic information via email and websites;
- Secure members-only access to information on the ISAC website;
- Conference calls for members; and
- Other IT such as pagers, telephone calls, and faxes to disseminate information.[84]

Eleven of the 15 existing ISACs have "created an ISAC Council to work on various operational, process, and other common issues to effectively analyze and disseminate information and, where possible, to leverage the work of the entire ISAC community," Dacey reported. He also provided examples of actions taken by DHS and other agencies to promote and support ISACs, organize critical infrastructure sectors, and foster information sharing through the ISACs.[85]

In a July 2004 followup report to the leaders of the two subcommittees of the House Select Committee on Homeland Security to whom testimony had been given

---

[82] U.S. White House Office, *Department of Homeland Security Reorganization Plan* (Washington: Nov. 25, 2002), p. 9.

[83] U.S. General Accounting Office, *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors*, GAO Testimony GAO-04-699T (Washington: Apr. 21, 2004), p. 2.

[84] Ibid., p. 16; Dacey noted that "the Telecommunications ISAC uses the Critical Infrastructure Warning Information Network," which provides continuous, around-the-clock alert and notification capability to government and industry participants.

[85] Ibid., pp. 23, 24-26.

earlier, GAO identified actions the Department of Homeland Security (DHS) and the ISACs could take to improve the effectiveness of CIP information sharing efforts. Among the more significant challenges identified were the following.

- Government agencies and the ISACs need to build trusted relationships between them to facilitate information sharing. In some cases, establishing such relationships may be difficult because sector-specific agencies may also have a regulatory role.

- The federal government and the private sector should share information on incidents, threats, and vulnerabilities. Most ISACs reported that they believed they were providing appropriate information to the government but, while noting improvements, they still had concerns with the information being provided to them by DHS and/or their sector-specific agencies. These concerns included the limited quantity of information and the need for more specific, timely, and actionable information. In its recent white papers, the ISAC Council also has identified a number of potential barriers to information sharing between the private sector and the government. These included the sensitivity of the information (such as law enforcement information), legal limits on disclosure (such as Privacy Act limitations on disclosure of personally identifiable information), and contractual and business limits on how and when information is disclosed (e.g., the Financial Services ISAC does not allow any governmental or law enforcement access to its database). The Council also emphasized that perhaps the greatest barriers to information sharing stem from practical and business considerations in that, although important, the benefits of sharing information are often difficult to discern, while the risks and costs of sharing are direct and foreseeable.

- The roles of the various government and private-sector entities involved in protecting critical infrastructures must continue to be identified and defined. In particular, officials for several ISACs wanted a better definition of DHS's role with respect to them. The ISAC Council also identified the need for DHS to establish the goals of its directorates and the relationship of these directorates with the private sector. The Council also wants clarification of the roles of the other federal agencies, state agencies, and other entities — such as the National Infrastructure Advisory Council.

- Government funding is needed. Ten of the ISACs we contacted emphasized the importance of government funding for purposes including creating the ISAC, supporting operations, increasing membership, developing metrics, and providing for additional capabilities.

- Private-sector analytical efforts should not be overlooked and must be integrated into the federal processes for a more complete understanding. The private sector understands its processes, assets,

> and operations best and can be relied upon to provide the required private-sector subject matter expertise.[86]

Acknowledging that "DHS has taken a number of actions to implement the public/private partnership called for by federal CIP policy," GAO, nonetheless, concluded:

> DHS has not yet developed a plan for how it will carry out its information sharing responsibilities, including efforts to address the challenges identified by the ISACs and the ISAC Council. In addition, DHS has not developed internal policies and procedures to help ensure effective information sharing by the many entities within the department that collect and analyze information that may impact the security of our nation's critical infrastructure. It is essential for DHS to develop this plan, along with internal policies and procedures, to establish effective information-sharing relationships both within DHS and with other federal agencies and infrastructure sectors.[87]

Legislative Considerations

It appears that there are at least two possible legislative approaches to create a policy framework for a trusted information network for sharing counterterrorism and related information among federal, state, and local governments, as well as selected portions of the private sector. One strategy might be to amend the Homeland Security Act with such a framework. Another strategy might be to amend Chapter 35 of Title 44, United States Code, captioned "Coordination of Federal Information Policy." Located in this chapter are such information life cycle management laws as the Paperwork Reduction Act and the Federal Information Security Management Act, which was enacted as Title III of the E-Government Act of 2002.[88]

Each strategy has implications for the designation of a principal manager of the resulting policy framework for a trusted information sharing network. Amending the Homeland Security Act in this regard suggests that the Secretary of Homeland Security or his designee from within the Department of Homeland Security, such as the Chief Information Officer, would be the principal network manager, while amending Chapter 35 of Title 44, United States Code, suggests the Director of the Office of Management and Budget (OMB) or his designee would be the principal manager. In the latter case, however, it might be possible that the OMB director would designate the Secretary of Homeland Security or another official within the Department of Homeland Security, with the Secretary's concurrence, as his agent for managing the network. Whether the OMB director or the Secretary of Homeland Security is made the principal manager of the network, it would probably be useful, in terms of accountability, to specify that a "principal officer" shall be designated by either the OMB director or the Secretary, as the case may be, whose primary

---

[86] U.S. General Accounting Office, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO Report GAO-04-780 (Washington: July 2004), pp. 9-10.

[87] Ibid., p. 10.

[88] 116 Stat. 2899 at 2946.

responsibility shall be to carry out the duties of whichever official is tasked as the principal manager.

Identified below are some possible components for legislation establishing a policy framework for a trusted information network for information sharing: purposes, definitions, authority and functions of a principal manager, federal agency responsibilities, other participants' responsibilities (which, at this basic stage of development, are the same as those set out for federal agencies), and annual inventory and assessment of information sharing initiatives.[89] Options regarding the primary manager are provided, and some other considerations are offered for each of the proffered components.

While some of the key recommendations of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) report emphasized the need to improve information sharing practices, the report was, for the most part, silent regarding how these recommendations might be carried out statutorily. To that end, legislation to implement the "trusted information network" called for in the 9/11 Commission report would need to address concerns such as standard-setting authority, agency responsibilities, and congressional oversight. The concepts set out below are possible components of potential information sharing legislation.

Purposes.

The purposes of this act are the following:

- To facilitate the creation of a "trusted information network."
- To promote better informed decisionmaking by policy makers.
- To improve the ability of the government to share information within and among agencies, and among federal, state, and local government agencies and selected portions of the private sector.
- To promote interoperable information standards.
- To facilitate a shift from a "need to know" culture of information protection to a "need to share" culture of integration.

Definitions.

- Director — the term "Director" means the Director of the Office of Management and Budget (OMB) [alternatively, the Secretary of Homeland Security may be inserted].
- Trusted information network — the term "trusted information network" means a secure, decentralized, scalable, interoperable,

---

[89] The Federal Information Security Management Act provides a legislative model at 116 Stat. 2946.

permission-based network, accessible to the appropriate federal, state, local, and private sector entities, designed to facilitate the sharing and analysis of information.

- Enterprise architecture — the term "enterprise architecture" means (A) (i) a strategic information asset base, which defines the mission; (ii) the information necessary to perform the mission; (iii) the technologies necessary to perform the mission; and (iv) the transitional processes for implementing new technologies in response to changing mission needs; and (B) includes (i) a baseline architecture; (ii) a target architecture; and (iii) a sequencing plan.

- Relevant agency — the term "relevant agency" means any agency with responsibility for intelligence and/or homeland security.

Authority and Functions of the OMB Director [or, Alternatively, the Secretary of Homeland Security].

The Director [or Secretary of Homeland Security], in coordination with the Secretary of Homeland Security [or omit in alternative case], the Chief Information Officer and the Chief Technology Officer of the Department of Homeland Security, and the designated representatives of the relevant agencies, and in accordance with the Clinger-Cohen Act of 1996 and the E-Government Act of 2002, shall:

- Endeavor to make the information technology systems of the federal government, including communications systems, effective, efficient, secure, and appropriately interoperable.

- Oversee and ensure the development and implementation of a trusted information network for government-wide information sharing.

- Develop, in conjunction with ongoing federal enterprise architecture efforts, a comprehensive enterprise architecture for information systems, including communications systems, to achieve interoperability between and among information systems of agencies with responsibility for homeland security.

- Develop a plan to achieve interoperability between and among information systems, including communications systems, of agencies with responsibility for homeland security and those of state and local agencies with responsibility for homeland security.

- Establish timetables for the development and implementation of the trusted information network and associated enterprise architecture.

- Consult with information systems management experts in the public and private sectors, in the development and implementation of the trusted information network and associated enterprise architecture.

- Submit, not later than 120 days after the enactment of this act, a report on efforts to develop and implement the trusted information network to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives, with semi-annual reports submitted thereafter.

- Designate, with the approval of the President, a principal officer in the Office of Management and Budget [or Department of Homeland Security], whose primary responsibility shall be to carry out the duties of the Director [or Secretary of Homeland Security] assigned in this act.

Federal Agency Responsibilities.

The head of each relevant agency shall:

- Cooperate fully with the Director [or Secretary of Homeland Security] in the development of the trusted information network and associated enterprise architecture to implement government-wide information sharing, and in the management and acquisition of information technology consistent with applicable law.

- Develop, document, and implement an agency-wide plan to participate in the trusted information network in accordance with any policies or procedures promulgated by the Director [or Secretary of Homeland Security].

- Report semi-annually to the Director [or Secretary of Homeland Security] on the progress and effectiveness of efforts to develop and adopt interoperable information standards, and a scalable enterprise architecture, and the scope and substance of the information being shared with other federal, state, and local agencies and selected portions of the private sector.

- Designate a chief information sharing officer whose primary responsibility shall be to carry out the agency's responsibilities related to this act in coordination with the Director [or Secretary of Homeland Security].

Other Participants' Responsibilities.

The head of each relevant state and local government agency, other governmental entity, or private sector organization shall:

- Cooperate fully with the Director [or Secretary of Homeland Security] in the development of the trusted information network and associated enterprise architecture to implement government-wide information sharing, and in the management and acquisition of information technology consistent with applicable law.

- Develop, document, and implement an agency-wide plan to participate in the trusted information network in accordance with any policies or procedures promulgated by the Director [or Secretary of Homeland Security].

- Report semi-annually to the Director [or Secretary of Homeland Security] on the progress and effectiveness of efforts to develop and adopt interoperable information standards, and a scalable enterprise architecture, and the scope and substance of the information being shared with other federal, state and local agencies and selected portions of the private sector.

- Designate a chief information sharing officer whose primary responsibility shall be to carry out the agency's responsibilities related to this act in coordination with the Director [or Secretary of Homeland Security].

Annual Inventory and Assessment of Information Sharing Initiatives.

- Each year the Director [or Secretary of Homeland Security] shall perform an inventory of existing information sharing initiatives being carried out at the federal, state, and local levels to assess what information is being shared, with whom it is being shared, resources being used, the effectiveness of the initiative, and to identify any overlap or duplication of efforts.

- For each initiative documented in the inventory, the inventory shall include information regarding: the lead agency/organization in charge of the initiative, the participant agencies involved in each initiative, the type(s) of information being shared, the technology used to facilitate sharing, the capabilities of the sharing system, and security procedures.

- To the extent an information sharing initiative includes classified activities, details about this initiative will be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

- Not later than 90 days after the date of enactment of this act, an initial inventory of information sharing initiatives shall be prepared by the Director [or Secretary of Homeland Security] and submitted to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives, with annual reports submitted thereafter.

Related Proposed Legislation

Among the information sharing proposals offered during the 108th Congress, S. 2701, the Homeland Security Interagency and Interjurisdictional Information Sharing

Act of 2004, was introduced by Senator Joseph Lieberman with bipartisan support on July 21, 2004.[90] Referred to the Committee on Governmental Affairs, the legislation would establish a Homeland Security Information Sharing Network to facilitate information flow within and among federal, state, local, and tribal government agencies; establish a Homeland Security Information Coordinating Council to develop and oversee protocols and procedures for sharing homeland security information; direct the Secretary of Homeland Security to create a performance management plan and an incentive program to assess and promote information sharing objectives; and establish an Office of Information Sharing (OIS) within the Office for State and Local Government Coordination and Preparedness at DHS. OIS, among other responsibilities, would be tasked with facilitating information sharing among federal, state, and local government agencies through the creation of regional task forces and the establishment of 24-hour operations centers in each state; fostering the development of interoperable communications systems for state and local agencies; providing technical assistance to state and local agencies in the development of regional information sharing networks; and administering a preparedness grant program to support state and local agency information sharing activities.

Senator Lieberman also introduced S. 2708, the National Strategy for Homeland Security Act of 2004, on July 21, 2004.[91] Referred to the Committee on Governmental Affairs as well, the measure directs the Secretary of Homeland Security, "in collaboration with the Assistant to the President for Homeland Security and the Homeland Security Council," to "develop the National Strategy for Homeland Security for the detection, prevention, protection, response, and recovery with regard to terrorist threats to the United States." This mandated national strategy would be an updated version of the one issued in July 2002, and would itself be rewritten every fours years, with updates every two years and annual progress reports to be submitted with the President's annual budget request. With respect to information sharing, Section 3(c)(2)(a) of S. 2708 would have the National Strategy for Homeland Security include "policies and procedures to maximize the collection, translation, analysis, exploitation, and dissemination of information relating to combating terrorism and the homeland security response throughout the Federal government, and with State and local authorities, and, as appropriate, the private sector."

On September 7, 2004, Senator John McCain, with bipartisan support, introduced S. 2774, the 9/11 Commission Report Implementation Act of 2004.[92] Read the first time and placed on the Senate legislative calendar, the measure includes provisions designed to implement most of the 41 recommendations offered in the 9/11 Commission report. Title II of the bill specifically addresses issues related to information sharing. Various provisions direct the President to establish an information sharing network to facilitate collaboration and information sharing among federal, state, local, and tribal government agencies; establish an Advisory

---

[90] *Congressional Record*, daily edition, vol. 150, July 21, 2004, pp. S8550-S855.

[91] Ibid., pp. S8558-S8559.

[92] Ibid., Sept. 7, 2004, pp. S8864-S8915.

Council on Information Sharing to advise the President and relevant agency officials on issues related to the establishment and ongoing operation of the information sharing network; require the President to submit semiannual reports to Congress regarding the state of the information sharing network; require participant agencies to submit annual reports to the Office of Management and Budget (OMB) regarding their use and expenditures related to the information sharing network; and require the Government Accountability Office (GAO) to assess periodically the implementation and operation of the information sharing network. A companion bill, H.R. 5040, was introduced in the House on September 9 by Representative Christopher Shays for himself and 32 cosponsors, and was referred to 10 committees.

A somewhat similar bill, H.R. 5024, was introduced in the House on September 8 by Representative Nancy Pelosi, the minority leader, with 109 initial cosponsors, and was referred to 11 committees. Title V of the proposal directs the President to determine guidelines for acquiring, accessing, using, and sharing information about individuals among federal, state, and local governments, as well as the private sector, and establishes "within the executive branch a board to oversee adherence to" the President's afore-mandated guidelines and "the commitment the Government makes to defend civil liberties."

Another comprehensive reform bill, S. 2811, introduced on September 15 by Senator Arlen Specter, establishes a Department of Intelligence headed by a Director of Intelligence.[93] Among other responsibilities, the director is to develop, in consultation with the Secretary of Defense, the Secretary of Homeland Security, and the heads of other appropriate departments and agencies, an integrated communications network that provides interoperable communications capabilities among all elements of the intelligence community and such other entities and persons as the director considers appropriate; set forth, after consultation with the Attorney General, common standards, through written requirements, procedures, and guidelines, for the collection and sharing of information collected abroad and in the U.S. by the elements of the intelligence community, and with state and local governments in consultation with the Secretary of Homeland Security, while to the maximum extent practicable, protecting the privacy and civil liberties of U.S. persons and ensuring the relevant officers of the federal government are provided with clear, understandable, consistent, effective, and lawful procedures and guidelines for the collection, handling, distribution, and retention of information; and require information to be shared free of originator controls, including controls requiring the consent of the originating agency prior to the dissemination of the information outside any other agency to which it has been made available, and otherwise minimizing the applicability of information compartmentalization systems to information while holding personnel accountable for increased sharing of intelligence related to the national security. The bill was referred to the Committee on Governmental Affairs.

On September 16, the Bush Administration sent to Congress draft legislation to strengthen the intelligence capabilities of the federal government. Based upon recommendations of the 9/11 Commission, the proposal establishes a National

---

[93] *Congressional Record*, daily edition, vol. 150, Sept. 15, 2004, p. S9288.

Intelligence Director (NID), who, among other responsibilities, is to establish common security and access standards for managing and handling intelligence systems, information, and products, including access to collected data and analytic products generated by or within the intelligence community, focusing particularly on facilitating among the agencies and organizations within the intelligence community and networks available across the other federal agencies involved in national security and homeland security activities, state and local governments, and, as appropriate, other entities, the fullest and most prompt sharing of and access to information and products practicable, including access to collected data and analytic products, with special emphasis on detecting, preventing, preempting, and disrupting terrorist threats and attacks against the U.S., its people, property, and interest. In doing so, the director is also tasked with the establishment of interface standards for an interoperable information-sharing enterprise that facilitates automated access to national intelligence by agencies and organizations within the intelligence community.

Selected by the Senate majority and minority leaders to lead the effort to legislatively implement the recommendations of the 9/11 Commission, Senator Susan Collins, the chair of the Committee on Governmental Affairs, and Senator Joseph Lieberman, the ranking minority member on the panel, initially discussed the general terms of their reform bill at a September 15 press conference.[94] The text of the legislation was made public in draft form on September 20. The Committee on Governmental Affairs began a markup of the Collins proposal on September 21, and completed their action the following day when the committee ordered the amended measure favorably reported as an original bill. Introduced by Senator Collins as an original bill on September 23, the legislation was designated S. 2840, the National Intelligence Reform Act.[95] The proposal was also introduced a second time that day, with Senator Lieberman as a cosponsor, and was designated S. 2545. At the end of the day, unanimous-consent agreement was reached providing that, on September 27, the Senate would begin consideration of S. 2845. As introduced, S. 2845 makes the NID responsible for intelligence dissemination and sharing, including using an integrated communications network that provides interoperable communications capabilities among all elements of the intelligence community and other appropriate entities; directs the President to establish a trusted information network to facilitate collaboration and information sharing among federal, state, local, and tribal government agencies; establishes an Advisory Council on Information Sharing to advise the President and relevant agency officials on issues related to the establishment and ongoing operation of the information sharing network; requires the President to submit semiannual reports to Congress regarding the state of the information sharing network; requires participant agencies to submit annual reports to OMB regarding their use and expenditures related to the information sharing network; and requires GAO to assess periodically the implementation and operation of the information sharing network. A bill very similar to S. 2845 was introduced in

---

[94] Amy Klamper and John Stanton, "Intelligence: ... As Collins, Lieberman Unveil a Rtesponse to 9/11 Panel," *CongressDailyPM*, Sept. 15, 2004, available at [http://nationaljournal.com/pubs/congressdaily/dj040915.htm]; Philip Shenon, "Intelligence Proposals Gain in Congress," *New York Times*, Sept. 16, 2004, p. A15.

[95] See *Congressional Record*, daily edition, vol. 150, Sept. 23, 2004, pp. S9615-S9638.

the House on September 24 by Representative Christopher Shays with bipartisan support and was designated H.R. 5150, the National Intelligence Reform Act. It was referred to the Permanent Select Committee on Intelligence.

In the House, the vehicle for implementing the recommendations of the 9/11 Commission was introduced by Representative Dennis Hastert on September 24 and was designated H.R. 10, the 9/11 Recommendations Implementation Act. The bill drew upon the President's September 16 draft proposal, with additional input from committee chairs who had held hearings on the findings and recommendations of the 9/11 Commission during August and the early weeks of September. As a result, the bill contains various provisions not found in S. 2845, as introduced. Provisions of H.R. 10, as introduced, vest the NID with authority to ensure maximum availability of, and access to, intelligence information within the intelligence community, consistent with national security requirements; authorize additional appropriations for information systems for sharing data concerning money laundering and terrorist financing;; foster improved information sharing and dissemination by the Federal Bureau of Investigation; direct the NID to establish an interim, interoperable intelligence data exchange system that will connect the data systems operated independently by the entities in the intelligence community and by the National Counterterrorism Center (NCTC) to permit automated data exchange among these entities, and also to establish a fully functional, interoperable law enforcement and intelligence electronic data system — to be known as the "Chimera system"— within the NCTC to provide immediate access to information in databases of federal law enforcement agencies and the intelligence community that is necessary to identify terrorists, and organizations and individuals that support terrorism; and mandate the Secretary of Homeland Security to establish a mechanism to ensure the coordination and dissemination of terrorist travel intelligence and operational information among appropriate agencies. The House bill was referred to the Committees on Armed Services, Education and the Workforce, Energy and Commerce, Financial Services, Government Reform, International Relations, the Judiciary, Rules, Science, Transportation and Infrastructure, and Ways and Means, as well as the Permanent Select Committee on Intelligence and the Select Committee on Homeland Security. Committee markups were scheduled to begin on September 29.

The perceived sense of urgency concerning legislation related to the recommendations of the 9/11 Commission appears to be strong. There are, however, relatively few legislative days remaining in the second session of the 108th Congress. In addition, the complexity of the issues involved, and other competing legislative priorities, such as appropriations, suggests that activity on information sharing legislation might be carried over to the 109th Congress. This could take the form of brief bills designed to amend or augment specific aspects of existing law, or attempts at early passage of a more comprehensive bill, which might have been discussed or debated in the closing days of the 108th Congress.

Appendix 1: Selected Online Information Sharing Resources

Lessons Learned Information Sharing (LLIS.gov)
[http://www.llis.gov]

Information Sharing and Analysis Center Council (ISAC Council)
[http://www.isaccouncil.org/]

Multi-State Information Sharing Analysis Center (MS-ISAC)
[http://www.cscic.state.ny.us/msisac/index.html]

Water Information Sharing and Analysis Center (WaterISAC)
[http://www.waterisac.org/]

Financial Services Information Sharing and Analysis Center (FS-ISAC)
[http://www.fsisac.com/]

Information Technology Information Sharing and Analysis Center (IT-ISAC)
[https://www.it-isac.org/index.php]

Energy Information Sharing and Analysis Center (ENERGY-ISAC)
[http://www.energyisac.com/index.cfm]

Electricity Sector Information Sharing and Analysis Center (ESISAC)
[http://www.esisac.com]

Chemical Sector Information Sharing and Analysis Center
[http://chemicalisac.chemtrec.com]

Healthcare Services Information Sharing and Analysis Center (HCISAC)
[http://www.hcisac.org]

Highway Information Sharing and Analysis Center
[http://www.truckline.com/insideata/isac/]

Surface Transportation and Public Transportation Information Sharing and Analysis Center (ST-ISAC)
[http://www.surfacetransportationisac.org/]

National Coordinating Center for Telecommunications Information Sharing and Analysis Center (NCC-ISAC)
[http://www.ncs.gov/ncc/main.html]