Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress

Mark A. Randol
Specialist in Domestic Intelligence and Counter-Terrorism

November 5, 2009

Congressional Research Service
7-5700
www.crs.gov
R40901

Summary

The 2004 National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) cited breakdowns in information sharing and the failure to fuse pertinent intelligence (i.e., "connecting the dots") as key factors in the failure to prevent the 9/11 attacks. Efforts undertaken since 2001 to tackle these issues include the following:

- Congress mandated the creation of an information-sharing environment (commonly known as the "ISE") that would provide and facilitate the means of sharing terrorism information among all appropriate federal, state, local, and tribal entities and the private sector through the use of policy guidelines and technologies.
- States and major urban areas established intelligence fusion centers to coordinate the gathering, analysis, and dissemination of law enforcement, homeland security, public safety, and terrorism intelligence and analysis.
- Various data mining programs were initiated in an effort to uncover terrorism plots. Data mining involves pattern-based queries, searches, or other analyses of one or more electronic databases.

The imperative for the exchange of terrorism-related intelligence information among law enforcement and security officials at all levels of government is founded on three propositions. The first is that any terrorist attack in the homeland will necessarily occur in a community within a state or tribal area, and the initial response to it will be by state, local, and tribal emergency responders and law enforcement officials. Second, the plotting and preparation for a terrorist attack within the United States (such as surveillance of a target, acquisition and transport of weapons or explosives, and even the recruitment of participants) will also occur within local communities. Third, "[i]nformation acquired for one purpose, or under one set of authorities, might provide unique insights when combined, in accordance with applicable law, with seemingly unrelated information from other sources."

Suspicious Activity Reports (SARs) contain information about criminal activity that may also reveal terrorist pre-operational planning. Many believe that the sharing of SARs among all levels of government and the fusing of these reports with other intelligence information will help uncover terrorist plots within the United States.

The Nationwide SAR Initiative (NSI) is an effort to have most federal, state, local, and tribal law enforcement organizations participate in a standardized, integrated approach to gathering, documenting, processing, and analyzing terrorism-related SARs. The NSI is designed to respond to the mandate of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), for a "decentralized, distributed, and coordinated [information sharing] environment ... with 'applicable legal standards relating to privacy and civil liberties.'"

This report describes the NSI, the rationale for the sharing of terrorism-related SARs, and how the NSI seeks to achieve this objective. It examines the privacy and civil liberties concerns raised by the initiative and identifies other oversight issues for Congress.

Contents

Figures

Appendixes

Contacts

Background

The 9/11 Commission cited breakdowns in information sharing and the failure to fuse pertinent intelligence (i.e., "connecting the dots") as key factors in the failure to prevent the 9/11 attacks.[1] A bipartisan task force[2] of former policy makers and senior executives described the challenge facing the government in "the new era of national security we have entered," as "the challenge of using information effectively, linking collection with sound and imaginative analysis derived from multiple perspectives, and employing cutting edge technology to support end-users, from emergency responders to Presidents. In other words, we need to *mobilize* information.... "[3]

Several efforts have been undertaken since 2001 to tackle these issues. In the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA), Congress mandated the creation of an Information Sharing Environment (commonly known as the "ISE").[4] Congress intended the ISE to be a "decentralized, distributed, and coordinated environment ... with 'applicable legal standards relating to privacy and civil liberties.'" The Act also directed that the ISE provide and facilitate the means of sharing terrorism information among all appropriate federal, state, local, and tribal entities and the private sector through the use of policy guidelines and technologies.[5]

A Program Manager for the Information Sharing Environment (PM-ISE) was established and placed within the Office of the Director of National Intelligence (ODNI). As required by Section 1016(h) of the IRTPA, the PM-ISE submitted to Congress three annual reports on the extent to which the ISE has been implemented.[6] The Obama Administration recently reaffirmed effective information sharing as a "top priority" and established within the Executive Office of the President the position of Senior Director for Information Sharing Policy.[7]

Also after 9/11, states and major urban areas established intelligence fusion centers to coordinate the gathering, analysis, and dissemination of law enforcement, homeland security, public safety, and terrorism intelligence and analysis.[8] Fusion centers have been defined as a "collaborative effort of two or more Federal, state, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity.... "[9] The Department

[1] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, July 22, 2004, pp. 353-356 and 416-418, available at http://www.9-11commission.gov. Hereafter: *9/11 Commission Report*.

[2] The Markle Task Force on National Security in the Information Age was convened to "recommend ways to improve national security decisions by transforming business processes and the way information is shared." The Task Force has published three reports: *Protecting America's Freedom in the Information Age*, October 2002; *Creating a Trusted Information Network for Homeland Security*, December 2003; *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*, July 2006. See Markle Foundation *Press Release*, March 10, 2009. These reports are available at http://www.markletaskforce.org/.

[3] Markle Task Force, *Protecting America's Freedom in the Information Age*, October 2002, p. 9. Hereafter: "Markle Report I."

[4] P.L. 108-458, Dec. 17, 2004, §1016(b), 118 STAT. 3665.

[5] Ibid.

[6] The latest report was submitted in June 2009 and is available at http://www.fas.org/irp/agency/ise/2009report.pdf.

[7] John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, Memorandum to Cabinet Principals, "Strengthening Information Sharing and Access," July 2, 2009.

[8] For background on state and local fusion centers, see CRS Report RL34070, *Fusion Centers: Issues and Options for Congress*, by John Rollins.

[9] P.L. 110-53, Aug. 3, 2007, §511, 121 STAT. 322. Amends *Homeland Security Act of 2002* by adding §210A(j).

of Homeland Security (DHS) cites 72 centers currently operational within the United States and its territories.[10] DHS has supported these centers with grant funding and assigned intelligence officers to them.

Post-9/11 efforts to "connect the dots" have included various data mining programs. Data mining is a type of database analysis that attempts to discover useful patterns or relationships in a group of data—particularly the discovery of previously unknown relationships—especially when derived from different databases.[11] Although data mining for counterterrorism purposes predated the 9/11 attacks,[12] it was considered a particularly promising tool after it was learned that certain database searches would have disclosed connections between Nawaf al Hazmi and Khalid al Midhar—the two 9/11 hijackers who were on a government terrorist watch list prior to September 11, 2001—with seven other hijackers hitherto unknown to the government.[13]

The Federal Bureau of Investigation's (FBI's) National Security Analysis Center (NSAC) maintains a collection of data sets with more than 1.5 billion government and private sector records about citizens and foreigners, according to documents recently obtained under the Freedom of Information Act.[14] A formerly secret 2008 funding justification among those released documents reportedly states that the "NSAC will also pursue 'pattern analysis' as part of its service to [the FBI National Security Branch]. Pattern analysis queries take a predictive model or pattern of behavior and search for that pattern in data sets. The FBI's efforts to define predictive models ... should improve efforts to identify 'sleeper cells.'"[15]

The effectiveness of data mining for counterterrorism and homeland security purposes has, however, been questioned by the scientific community, and privacy and civil liberties concerns have been raised. A study funded by DHS and conducted by a committee of the National Research Council[16] concluded that

> [m]odern data collection and analysis techniques have had remarkable success in solving information-related problems in the commercial sector; for example, they have been successfully applied to detect consumer fraud. But such highly automated tools and techniques cannot be easily applied to the much more difficult problem of detecting and preempting a terrorist attack, and success in doing so may not be possible at all.[17]

---

[10] U.S. Congress, Senate Homeland Security and Governmental Affairs Committee, *Eight Years After 9/11: Confronting the Terrorist Threat to the Homeland*, Written Statement of Secretary of Homeland Security, Janet Napolitano, 111th Cong., 1st sess., September 30, 2009.

[11] TheFreeDictionary at http://encyclopedia2.thefreedictionary.com/Data+mining">Data mining.

[12] For a discussion of data mining and homeland security including specific government data mining programs, see CRS Report RL31798, *Data Mining and Homeland Security: An Overview*, by Jeffrey W. Seifert. Hereafter: Seifert, CRS Report RL31798.

[13] For a description of these connections, see Markle Report I, p. 28.

[14] Ryan Singel, "Newly Declassified Files Detail Massive Data Mining Project," *Wired.com*, September 23, 2009, available at http://www.wired.com/threatlevel/2009/09/fbi-nsac/.

[15] Ibid.

[16] Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals. The Committee consisted of 21 people with a broad range of expertise in the scientific, government, and private sector communities. It was co-chaired by former Defense Secretary William J. Perry and Charles M. Vest of the National Academy of Engineering.

[17] National Research Council of the National Academies, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment* (Washington, DC: National Academies Press, 2008), p. 2.

Certain government data mining programs—such as the Defense Advanced Research Projects Agency's Total Information Awareness (TIA) program[18] and the Transportation Security Administration's Computer Assisted Passenger Prescreening System II(CAPPS II)—have been abandoned.[19] And Congress, in the Federal Agency Data Mining Reporting Act of 2007 (§804 of P.L. 110-53), has mandated detailed reporting requirements and privacy and civil liberties impact assessments for future data mining programs contemplated by federal agencies.

The FBI is seeking approval to expand the NSAC's capabilities.[20] It does not consider the NSAC a data mining program, but rather an "analysis center." It goes on to say that "any data mining that may be conducted, the majority of which is subject-based, is only a subpart of individual NSAC initiatives and not its overall mission.... The 2008 funding submission [one of the FBI documents obtained by *Wired.com* under the Freedom of Information Act], which indicates that NSAC would provide a pattern-based or predictive model, is now outdated and inaccurate."[21] The FBI also maintains that as a national security system, the NSAC would be exempt from the requirement for a privacy impact assessment (PIA).[22] But as a matter of policy, the FBI does PIA's for its national security systems, and one has been completed on the NSAC.[23]

Why Information Sharing?

> Information sharing is ... about establishing a collaborative environment with a clear purpose: ensuring that the right people have access to the right information at the right time under the right conditions to enable informed decisions.[24]

The imperative for the exchange of terrorism-related intelligence information among law enforcement and security officials at all levels of government is founded on three propositions:

The first is that any terrorist attack in the homeland will necessarily occur in a community within a state or tribal area, and the initial response to it will be by state, local, and tribal emergency responders and law enforcement officials.

Second, the plotting and preparation for a terrorist attack within the United States (such as surveillance of a target, acquisition and transport of weapons or explosives, and even the recruitment of participants) will also occur within communities. Every day, officers at more than 17,000 state and local law enforcement agencies collect and document information regarding behaviors, incidents, and other suspicious activity associated with crime including terrorism.[25] A

[18] For more information on this program, see CRS Report RL31730, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws*, by Gina Stevens, and CRS Report RL31786, *Total Information Awareness Programs: Funding, Composition, and Oversight Issues*, by Amy Belasco.

[19] Seifert, CRS Report RL31798, p. 4.

[20] FBI briefing to CRS, November 3, 2009.

[21] Ibid.

[22] P.L. 107-347, December 17, 2002, §208(b)(1)C., 116 STAT. 2922.

[23] FBI briefing to CRS, October 30, 2009.

[24] Markle Task Force, "Nation At Risk: Policy Makers Need Better Information to Protect the Country," March 2009, p. 3.

[25] *Findings and Recommendations of the SAR Support and Implementation Project, Final Draft*, June 2008, p. 6. The SAR Support and Implementation Project was a joint effort of the Department of Justice (DOJ) Bureau of Justice Assistance; the Major Cities Chiefs Association, DOJ's Global Justice Information Sharing Initiative (Global), the (continued...)

joint study by the Departments of Justice and Homeland Security and senior law enforcement officials concluded that "[t]he gathering, processing, reporting, analyzing, and sharing of suspicious activity is critical to preventing crimes, including those associated with domestic and international terrorism."[26]

Third, "[i]nformation acquired for one purpose, or under one set of authorities, might provide unique insights when combined, in accordance with applicable law, with seemingly unrelated information from other sources."[27] This recognizes that "relevant information comes from a much wider range of sources … and it is difficult to know *a priori* what information will prove relevant to analysts or useful to users. For this reason, it is necessary to create a more horizontal, cooperative, and fluid process for intelligence collection, sharing, and analysis."[28] Or, as the 9/11 Commission concluded, "A 'smart' government would *integrate* all sources of information to see the enemy as a whole."[29]

Information-Sharing Systems

In a nationwide survey conducted in 2006, the Justice Research and Statistics Association (JRSA) found that there are currently in place or under development 266 separate systems that share information about crime, including terrorism, at the national, regional, and state levels.[30] The boom in the development of these systems has led to concern that "it is hard to know what information is being shared and who is sharing it. In many cases, multiple systems are being developed to cover overlapping areas."[31] **Appendix A** provides a brief overview of significant information-sharing systems.

Suspicious Activity Reporting

Suspicious Activity Reports (SAR) contain information about criminal activity that may also reveal terrorist pre-operational planning.[32] These reports could be based on an officer's

(...continued)

Criminal Intelligence Coordinating Council, and DHS to develop recommendations to be used by law enforcement agencies to improve identification and reporting of suspicious activity and the sharing of that information with fusion centers and Joint Terrorism Task Forces. See pp. 1-2.

[26] Ibid., p. 2.

[27] National Strategy for Information Sharing, October 2007, pp. 2-3.

[28] Markle Report I, p. 48.

[29] 9/11 Commission Report, p. 401.

[30] The Justice Research and Statistics Association (JRSA), *Information Sharing Systems: A Survey of Law Enforcement*, July 31, 2006, p. 6. For a list of these systems, see Appendix B of the survey. The JRSA, founded in 1974, is a national nonprofit organization of state Statistical Analysis Center directors, researchers, and practitioners throughout government, academia, and criminal justice organizations.

[31] Ibid., p. 4.

[32] The term "suspicious activity report" is used in many contexts to describe behavior or activity that may be associated with crime, terrorism included. Another example of the use of the term is in connection with the Department of the Treasury's requirement that certain financial institutions file reports of "any suspicious transaction relevant to a possible violation of law or regulation." 31 U.S.C., Section 1818(g)(1). The requirement to file reports of suspicious transactions applies to some financial institutions, including banks, thrifts, credit unions, insurance companies, casinos, mutual funds, futures commission merchants, securities brokers and dealers, and money services businesses.

observation of suspicious behavior, 9-1-1 calls, or other tips and leads provided to police by citizens. Many believe that the sharing of SARs among all levels of government and combining them with other intelligence information will help uncover terrorist plots within the United States. Every day, more than 800,000 police officers collect and document information regarding behaviors, incidents, and other suspicious activity associated with crime, including terrorism.

"On the beat or mobile, cops are sensitive to things that do not look right or do not sound right," says one police chief. "[R]emember, it was a rookie cop on a routine check that resulted in the arrest of Eric Robert Rudolph in North Carolina despite the enormous commitment of federal resources."[33] Oklahoma City bomber Timothy McVeigh was arrested after a traffic stop when Oklahoma State Trooper Charles J. Hanger noticed that McVeigh's yellow 1977 Mercury Marquis had no license plate.[34] Using his home state as an example, a former U.S. Attorney maintains that "evidence of a potential terrorist threat or organized criminal enterprise is far more likely to be found in the incidental contact with the 10,000 police officers in the state of Washington than by the less than 150 FBI agents assigned to the Seattle Field Division."[35]

In addition to the arrests of Rudolph and McVeigh, state and local law enforcement officers, in the normal course of their duties, have uncovered or disrupted the following terrorist plots:

- The Japanese Red Army terrorist, Yū Kikumura, was arrested on April 12, 1988, at a rest stop on the New Jersey Turnpike by a state trooper who thought he was acting suspiciously. He was found carrying three 18-inch (46-cm) pipe bombs loaded with gunpowder. Prosecutors said Kikumura had planned to bomb a military recruitment office in New York City.[36]
- In July 2005, two undercover police officers noticed two men acting suspiciously near a gas station in Torrance, CA. After the men robbed the gas station, they were arrested by the undercover officers. A search of the arrested men's apartment revealed that they were members of the terrorist group Jamiyyat Ul-Islan Is-Saheeh. They were planning to bomb synagogues in Los Angeles and were financing their operation through armed robberies.[37]

---

[33] U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Homeland Security Intelligence: Its Relevance and Limitations*, Statement of John W. Gaissert, Chief of Police; Commerce, Georgia, 111th Cong., 1st sess., March 18, 2009.

[34] Trooper Hanger had no reason to suspect a connection between McVeigh and the bombing in Oklahoma City. But the trooper's suspicions were raised when the driver looked at his bumper when told why he had been pulled over. Says Trooper Hanger: "I thought if he knew he didn't have a tag, why did he look at the back of the car like that? It just didn't seem right." In addition, McVeigh was unable to provide proof of insurance and a bill of sale for the vehicle and then disclosed that he had a firearm. Trooper Hanger arrested McVeigh for five misdemeanors and took him into custody. McVeigh was awaiting arraignment when the FBI connected him to the bombing. See National Law Enforcement Officers Memorial at http://www.nleomf.com/TheFund/programs/OOM/hanger_oct01.htm.

[35] U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *A Report Card on Homeland Security Information Sharing*, Statement of John McKay, Former U.S. Attorney for the Western District of Washington, 110th Cong., 2nd sess., September 24, 2008. Hereafter: McKay Testimony, September 24, 2008.

[36] DOJ Office of the Inspector General Special Report, "The FBI Laboratory: An Investigation into Laboratory Practices and Alleged Misconduct in Explosives-Related and Other Cases," Section H2, Yū Kikumura Factual Background, April 1997.

[37] James Jay Carafano, "U.S. Thwarts 19 Terrorist Attacks Against America Since 9/11," Heritage Foundation, Backgrounder #2085, November 13, 2007.

- In August 4, 2007, two Egyptians studying in Florida were stopped by police for a traffic violation near Goose Creek, SC. They were found to have explosives in their vehicle. A subsequent investigation revealed that one of the students had made and placed on the Internet a video demonstrating how to use a doll to conceal an improvised explosive device. The student later plead guilty to "providing material support to terrorism."[38]

One major city police department commander notes that the role of police officers has evolved after 9/11. They are now also "first preventers" of terrorism, and this represents a "dramatic paradigm shift," both for the federal government and for the local and state agencies themselves.[39] The need for intelligence information to support the police in this terrorism prevention role is considered crucial. According to the Chair of the House of Representatives subcommittee concerned with these issues, "That's what 'homeland security intelligence' is all about: getting accurate, actionable, and timely information to the officers in our hometowns so they know who and what to look for in order to prevent the next 9/11."[40]

A national information-sharing system, says a former U.S. Attorney, should also ensure that "federal agencies have access to information maintained in state and local agencies that may be pertinent to terrorist threats ... the benefit that would accrue to U.S. national security in having police records integrated in a strictly controlled fashion with sensitive federal data would be nothing short of remarkable."[41] He cites the example of Hani Hanjoor, the hijacker who piloted American Airlines Flight 77 that crashed into the Pentagon. Six weeks prior to the 9/11 attacks, Hanjoor had been issued a speeding ticket by a local police department in the Washington, DC, area. Had a system been in place to share this information with the FBI, it may have alerted them that a suspected al-Qa'ida operative was present within the National Capital Region. Also prior to September 11, 2001, local police officers made separate traffic stops of two other 9/11 hijackers—Mohammed Atta and Ziad Samir Jarrah. Like Hanjoor, both were in violation of their immigration status. There was even an outstanding arrest warrant on Atta for failing to appear on a previous traffic citation.[42]

[38] St. Petersburg Times, "USF Terror Suspect Agrees to Plead Guilty," June 14, 2008, at http://tampabay.com/news/courts/criminal/article624049.ece.

[39] U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Homeland Security Intelligence: Its Relevance and Limitations*, Statement of Joan T. McNamara, Assistant Commanding Officer, Counter Terrorism and Criminal Intelligence Bureau, Los Angeles Police Department, 111th Cong., 1st sess., March 18, 2009. Hereafter: McNamara Testimony, March 18, 2009.

[40] Ibid., Opening Statement of Jane Harman; Chair, Subcommittee on Information Sharing, Intelligence, and Risk Assessment.

[41] McKay Testimony, September 24, 2008.

[42] See *9/11 and Terrorist Travel, Staff Report of the National Commission on Terrorist Attacks on the United States*, August 21, 2004, p. 139. Atta, who piloted American Flight 11, the first plane to hit the World Trade Center, was stopped on April 26, 2001, near Tamarac, FL, and cited for driving without a license. After he failed to appear in court on this citation, a warrant was issued for his arrest. On July 5, 2001, a Delray Beach, Florida police officer stopped Atta for speeding but gave him only a warning. See "The Road to Ground Zero, Part Five: A Trail of Missed Opportunities," *The Sunday Times*, February 3, 2002, at http://s3.amazonaws.com/911timeline/2002/sundaytimes020302.html. Ziad Samir Jarrah, who was believed to have piloted United Flight 93 that crashed in Pennsylvania, was pulled over by Maryland state troopers two days before the attacks while speeding on Interstate 95. See CNN.com "Maryland Police Release Hijacker Traffic Stop Video," January 8, 2002, at http://archives.cnn.com/2002/US/01/08/inv.hijacker.video/index.html.

Nationwide Suspicious Activity Reporting Initiative (NSI)

The NSI is a framework to support the reporting of suspicious activity—from the point of initial observation to the point where the information is available in the information-sharing environment.[43] It supports one of the core principles of the 2007 *National Strategy for Information Sharing*, that information sharing "be woven into all aspects of the counterterrorism activity, including preventive and protective actions, actionable responses, criminal and counterterrorism investigative activities, event preparedness, and response to and recovery from catastrophic events."[44] The NSI responds to the Strategy's mandate that the federal government support the development of a nationwide capacity for a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing information about suspicious activity that is potentially terrorism-related while protecting the privacy and civil liberties of Americans.[45]

According to the PM-ISE, the NSI is neither a technology nor a single, monolithic program. Rather it is a coordinated effort that integrates all SAR-related activities into a nationwide unified process.[46] The NSI is a framework that defines the data standards, business processes, and policies that facilitate the sharing of terrorism-related SARs.

The NSI also differs from data mining programs. Data mining entails the search of numerous commercial or government data sets that contain data—the vast majority of which documents legal activity. Mathematical algorithms are then used to identify data trends that can be examined as predictors of criminal activity. The NSI establishes a federated search[47] capability that requires the articulation of some type of criminal or law enforcement predicate before permitting a search of repositories consisting of documented events that are themselves considered reasonably indicative of criminal activity. Given the controversies surrounding various data mining programs,[48] this difference may be a salient issue in terms of public acceptance of the NSI program.

[43] NSI Project Overview Briefing by Russ Porter, Chairman of the Criminal Intelligence Coordinating Council of the Global Justice Information Sharing Initiative.

[44] National Strategy for Information Sharing, October 2007, p. 3.

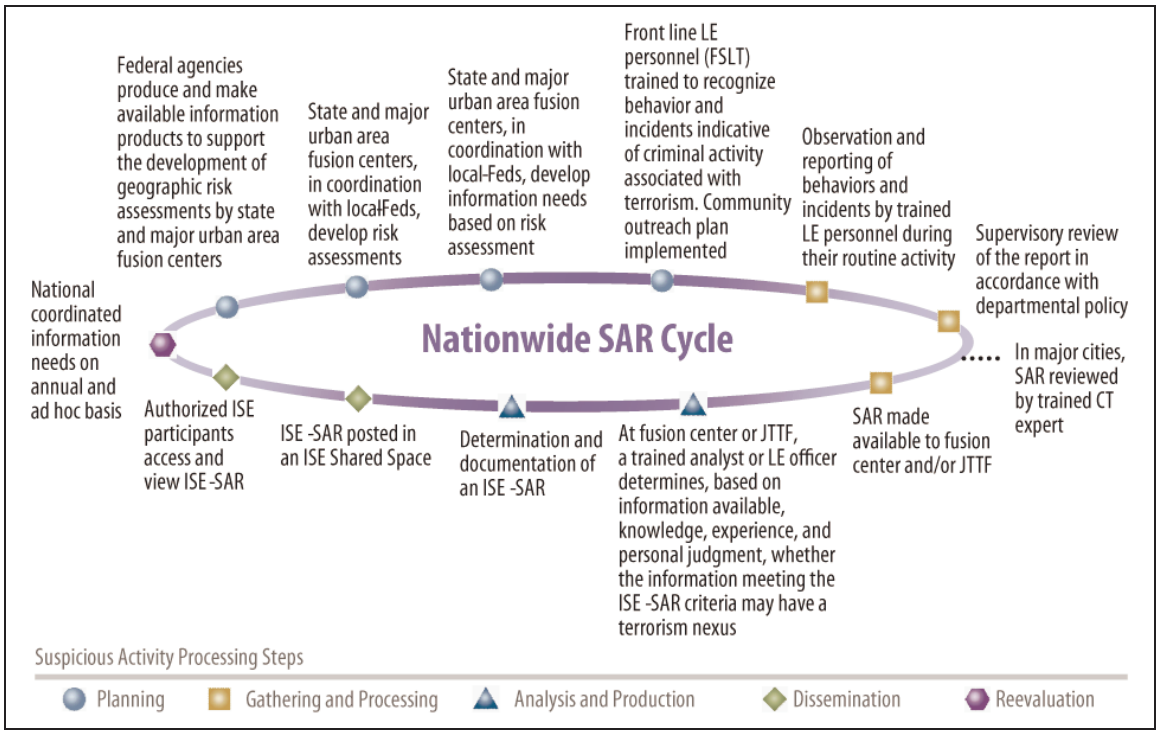
[45] See Ibid., p. A1-6, and PM-ISE, *Fact Sheet: Nationwide Suspicious Activities Reporting Initiative*, December 23, 2008, p. 1, at http://www.ise.gov/docs/sar/Fact_Sheet_NSI_-_December_23_2008_Final.pdf.

[46] Ibid.

[47] Federated search is the process of performing a simultaneous real-time search of multiple diverse and distributed sources from a single search page, with the federated search engine acting as intermediary. See Sol Lederman, "A Federated Search Primer, Part II," at http://www.altsearchengines.com/2009/01/12/a-federated-search-primer-part-ii-of-iii/

[48] Examples of this controversy can be found at Alice Lipowicz, "DHS' data mining sparks more controversy," *Federal Computer Week*, December 4, 2007, at http://fcw.com/articles/2007/12/04/dhs-data-mining-sparks-more-controversy.aspx; Susan Page, "NSA secret database report triggers fierce debate in Washington," *USA Today*, May 11, 2006, at http://www.usatoday.com/news/washington/2006-05-11-nsa-reax_x.htm; and William Safire, "You are a Suspect." *New York Times*, November 14, 2002, at http://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.html. See also Jeffrey A. Hart, "The Controversies over Data Mining and Warrantless Searches in the Wake of September 11," paper prepared for a panel on "Information Access, Power, and Rights," at the annual meeting of the International Studies Association, March 2008.

Figure 1. Nationwide Suspicious Activity Reporting (SAR) Cycle



Source: Program Manager for the Information Sharing Environment (PM-ISE).

In December 2008, a concept of operations for the NSI program was published that describes the roles, missions, and responsibilities of NSI participating agencies and the top level NSI governing structure. [49] A comprehensive overview of the operational steps of the nationwide SAR cycle grouped into five business process activities—planning, gathering and processing, analysis and production, dissemination, and reevaluation—is shown in **Figure 1**.

The intended operational steps of the cycle can be described simply: When a police officer detects suspicious activity that might be terrorist related, he or she documents that activity in a SAR. That report is reviewed within the officer's chain of command. Once vetted, it is submitted to a state/local fusion center, where it is reviewed by an intelligence analyst to determine whether it meets the established SAR criteria. If so, the report is entered into the information-sharing environment, where it becomes accessible to authorized agencies at all levels of government and available for analysis and fusion with other intelligence information.

Privacy and Civil Liberties Implications

According to the commander responsible for the Los Angeles Police Department (LAPD) SAR program, a suspicious activity reporting program should be "built upon behaviors and activities that have been historically linked to preoperational planning and preparation for terrorist attacks." Appropriately managed, a SAR program "takes the emphasis off the racial or ethnic

[49] PM-ISE, *Nationwide SAR Initiative Concept of Operations*, December 2008. p. 3, at http://www.ise.gov/docs/sar/NSI_CONOPS_Version_1_FINAL_2008-12-11_r5.pdf.

characteristics of individuals and places it on detecting behaviors and activities with potential links to terrorism related criminal activity."[50]

Some observers, however, are concerned that many behaviors that the police observe, and then use to judge whether the behaviors might be precursors to terrorism, are often entirely innocent and perfectly legal. Consider the following behaviors derived from the LAPD list of SAR "suspect actions":[51]

- Uses binoculars or cameras.
- Takes measurements.
- Takes pictures or video footage.
- Draws diagrams or takes notes.
- Pursues specific training or education that indicate suspicious motives (flight training, weapons training, etc).
- Espouses extremist views.

The American Civil Liberties Union (ACLU) argues that "[m]ost people engage in one or more of these activities on a routine, if not daily, basis." They fear that "overbroad reporting authority gives law enforcement officers justification to harass practically anyone they choose, to collect personal information, and to pass such information along to the intelligence community."[52] The Center for Democracy and Technology (CDT) is concerned that "there is a trend toward the collection of huge quantities of information with little or no predicate through SARs. There seems to us a high risk that this information will be misinterpreted and used to the detriment of innocent persons."[53]

In support of this contention, both the ACLU and CDT cite a case reported by the *Baltimore Sun* in July 2008: "Undercover Maryland State Police officers [in 2005 and 2006] ... sent covert agents to infiltrate the Baltimore Pledge of Resistance, a peace group; the Baltimore Coalition Against the Death Penalty; and the Committee to Save Vernon Evans, a death row inmate."[54] The police "also entered the names of some in a law-enforcement database of people thought to be terrorists or drug traffickers." According to files obtained by the ACLU through a Maryland Information Act lawsuit, "none of the 43 pages of summaries and computer logs—some with agents' names and whole paragraphs blacked out—mention criminal or even potentially criminal acts, the legal standard for initiating such surveillance."[55]

[50] McNamara Testimony, March 18, 2009.

[51] LAPD, "Terrorism Related Consolidated Crime and Analysis Database (CCAD) Codes," provided to CRS by the LAPD Counter-Terrorism and Criminal Intelligence Bureau, October 27, 2009.

[52] Mike German and Jay Stanley, American Civil Liberties Union, *Fusion Center Update*, July 2008, p. 2.

[53] U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Homeland Security Intelligence: Its Relevance and Limitations*, Statement of Gregory T. Nojeim, Director on Freedom, Security, and Technology, Center for Democracy and Technology, 111th Cong., 1st sess., March 18, 2009. Hereafter: Nojeim Testimony, March 18, 2009.

[54] Nick Madigan, "Spying Uncovered," *Baltimore Sun*, July 18, 2008, at http://www.baltimoresun.com/news/local/bal-te.md.spy18jul18,0,3787307.story.

[55] Ibid.

A challenge for the NSI is how to achieve law enforcement and intelligence objectives while ensuring privacy and civil liberties protections for American citizens. For example, all of the behaviors listed by the LAPD could be potential indicators of terrorist planning and preparation. But such behaviors could also be innocent and legal activities. Carefully articulating what activity crosses the threshold into reportable suspicious activity is seen as a necessary step to ensuring the protection of privacy and civil liberties.

ISE SAR Functional Standard

In an effort to address the privacy and civil liberties issues associated with the NSI, the PM ISE published a *ISE SAR Functional Standard*, which describes the structure, content, and products associated with processing, integrating, and retrieving SARs by participating agencies.[56] It is specifically intended to establish a structured environment to reduce inappropriate police data gathering and support the training of law enforcement personnel so that they can better distinguish between behavior that is legal or constitutionally protected and that which is potentially associated with criminal activity. It establishes threshold criteria for what suspicious activity will be considered as having a nexus to terrorism and establishes a two-step process to determine whether reports of that activity meet the criteria for being entered into the ISE as a SAR.

In 2008, the PM ISE completed a report that examined the potential impact of the *ISE SAR Functional Standard* on the privacy and other legal rights of Americans, how it will be evaluated in a limited operational environment, and articulated the measures that will be established to protect privacy and civil liberties.[57] Subsequently, the Office of the PM-ISE engaged with various stakeholders, including privacy and civil liberties groups such as the ACLU, CDT, and the Freedom and Justice Foundation, as it developed and refined SAR-related operational processes and training.[58] In May 2009, the suggestions of these groups as well as state and local law enforcement agencies were incorporated into a revised version of the *ISE SAR Functional Standard*.[59] Among the changes in the revision (Version 1.5) were the following:[60]

- Refines the definition of "suspicious activity," as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."
- Further emphasizes a behavior-focused approach to identify suspicious activity and requires that factors such as race, ethnicity, national origin, or religious affiliation should not be considered factors that create suspicion.

[56] PM ISE, *Fact Sheet: SAR Functional Standard in the ISE*, p. 3, at http://www.ise.gov/docs/ctiss/FactSheetCTISS_ISE-SAR.pdf.

[57] PM ISE, *Initial Privacy and Civil Liberties Analysis of the ISE-SAR Functional Standard and Evaluation Environment*, September 2008—Version 1. Hereafter: Initial Privacy and Civil Liberties Analysis of the ISE-SAR Functional Standard, September 2008, at http://www.ise.gov/docs/sar/.ISE_SAR_Initial_Privacy_and_Civil_Liberties_Analysis.pdf

[58] Office of the PM-ISE briefing to CRS, July 20, 2009.

[59] PM-ISE, *Information Sharing Environment Functional Standard Suspicious Activity Reporting, Version 1.5*, May 21, 2009, at http://www.ncirc.gov/sar/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued.pdf.

[60] PM ISE, Fact Sheet: Update to Suspicious Activity Reporting Functional Standard Provides Greater Privacy and Civil Liberties Protections, May 21, 2009, p. 1, at http://www.ise.gov/docs/ctiss/ISE-SAR_Functional_Standard_V1_5_Fact_Sheet.pdf.

- Refines the guidance to distinguish between Defined Criminal Activity and Potentially Criminal or Non-Criminal Activity requiring additional factual information before investigation.
- Clarifies those activities that are generally First Amendment-protected and should not be reported in a SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is reasonably indicative of criminal activity associated with terrorism.

In a press release following publication of Version 1.5, the ACLU National Security Policy Counsel noted that

> [t]he revised guidelines for suspicious activity reporting establish that a reasonable connection to terrorism or other criminal activity is required before law enforcement may collect Americans' personal information and share it within the ISE. These changes to the standard, which include reiterating that race cannot be used as a factor to create suspicion, give law enforcement the authority it needs without sacrificing the rights of those it seeks to protect. [61]

NSI Pilot Project

In 2007, the Office of the PM-ISE funded a pilot effort called the "ISE-SAR Evaluation Environment" (ISE-SAR EE) to evaluate the feasibility of the NSI for the sharing of terrorism-related SARs.[62] Program management services for the project were provided by the DOJ's Bureau of Justice Assistance (BJA) [63] with the support of the Global Justice Information Sharing Initiative (Global).[64]

The ISE-SAR EE sought to develop and implement consistent national policies, processes, and best practices among the federal, state, local, and tribal partners in the NSI initiative. System evaluations and training activities were conducted at three state and nine urban fusion centers pilot sites.[65] That evaluation program concluded on September 30, 2009. There were two specific activities of note within the ISE-SAR EE. First, the project team furnished and tested an operational technical infrastructure, referred to as the "shared spaces" concept, that would allow individual agencies to retain and control their own SAR data while making it easily and securely

[61] ACLU, Press Release, "Intelligence Community Raises Its Standards For Information Collection: Collaborative Effort Addresses Privacy and Civil Liberties Concerns," May 22, 2009, http://www.aclu.org/safefree/general/39656prs20090522.html.

[62] Office of the PM-ISE briefing to CRS, July 20, 2009.

[63] BJA, a component of DOJ's Office of Justice Programs, supports law enforcement, courts, corrections, treatment, victim services, technology, and prevention initiatives that strengthen the nation's criminal justice system. Among its activities, BJA provides technical advice and assistance to states and major urban areas on the development of their intelligence fusion centers. See DOJ *Global Justice Information Sharing Initiative*, 2009, p. 6.

[64] Global brings stakeholders together in five major working groups to collaborate on major information sharing challenges. The working groups are Global Infrastructure/Standards, Criminal Intelligence Coordinating Council, Global Intelligence, Global Privacy and Information Quality, and Global Security. See Ibid.

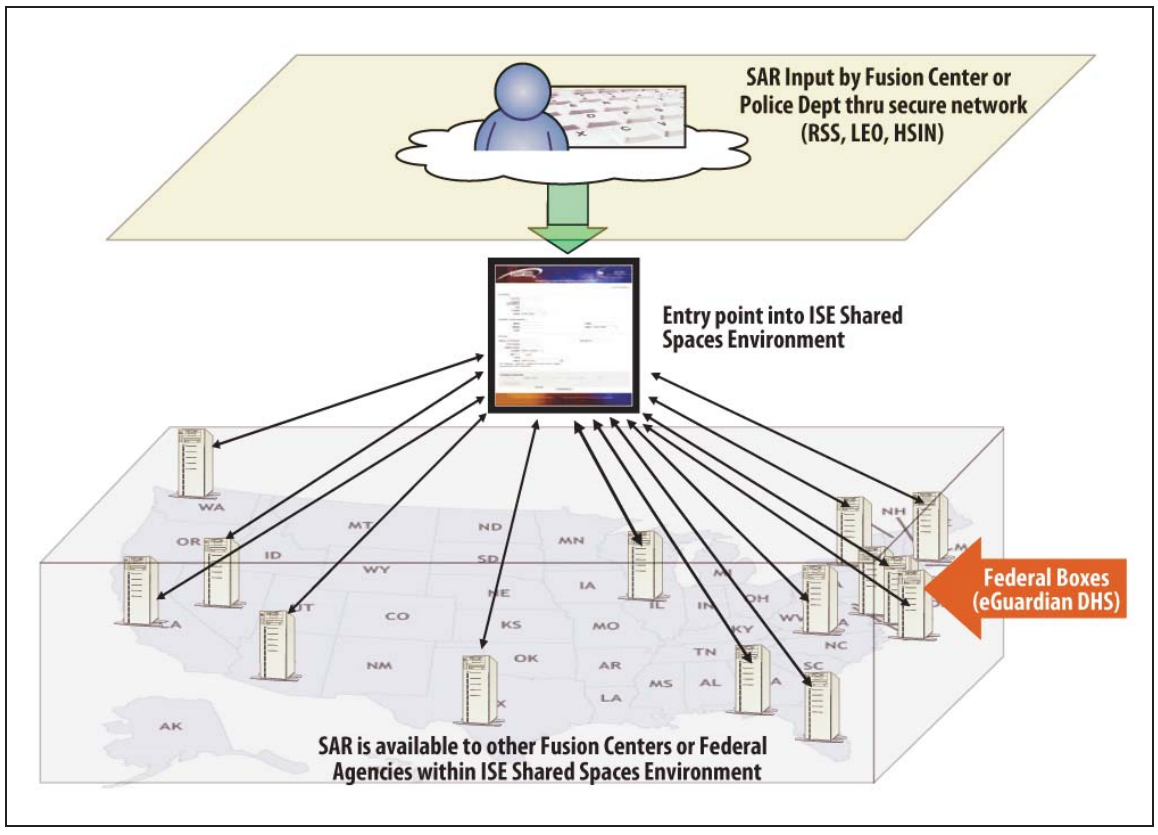
[65] Pilot sites are the Police Departments of Boston, Chicago, Houston, Las Vegas, Los Angeles, Miami-Dade, and Washington DC; Arizona Department of Public Safety (Arizona Counterterrorism Information Center), Florida Department of Law Enforcement, New York State Intelligence Center, Seattle Police Department/Washington State Fusion Center, and the Virginia Fusion Center.

accessible to authorized users among partner agencies. Second, a pilot training program was developed for the thousands of state and local law enforcement officers to assist them in the detection, identification, and reporting of suspicious activity in a way that supports the analysis and fusion of such reports into actionable intelligence while protecting privacy and civil liberties.

ISE Shared Spaces Architecture[66]

In order for state and local fusion centers to have access to each other's information as well as to the appropriate federal databases, the NSI uses a "shared spaces" architecture. Under this concept, the fusion centers replicate data from their systems to an external server under their control, which allows them to decide which information to share. A secure portal is then created that allows simultaneous searching of all such databases so that fusion centers will be able to aggregate any relevant information that exists throughout the national fusion center network. (See **Figure 2**.) The NSI evaluation project team arranged for secure access to this portal on one of three existing networks—Law Enforcement Online, Regional Information Sharing Systems Program, and Homeland Security Information Network.[67]

Figure 2. ISE SAR "Shared Spaces" Concept



Source: DOJ, Bureau of Justice Assistance.

[66] Information about NSI information technology infrastructure requirements provided by Paul Wormeli, Executive Director of the IJIS Institute.

[67] See **Appendix A** for a description of these systems.

FBI's *eGuardian* system[68] is a node of within the ISE Shared Spaces environment. On the surface, it would appear that the existing *eGuardian* capability duplicates the NSI—or at least NSI's shared spaces concept. But it should be noted that the NSI is an overall framework for a SAR process that includes policies, governance, procedures, training, and information technology (IT) architecture, whereas *eGuardian* is a specific technology for terrorism-related information sharing.

Under NSI, *eGuardian* can remain the technology that FBI uses to supply data to and access data from the ISE Shared Spaces environment. Likewise, fusion centers or state and local governments may, if they wish, use *eGuardian* as its gateway to and from the shared spaces. However, some law enforcement agencies may choose, or are legislatively mandated, to maintain a repository of their own data and to control what data is shared with whom based on statutory criteria. Consistent with the requirement in the IRTPA for a "decentralized, distributed, and coordinated" information-sharing environment, the NSI shared spaces architecture allows state, local, and tribal agencies to maintain control of their own data.

Training

The NSI project team recognized that training is a key element of the SAR process—for front line personnel, for their supervisors, and for intelligence analysts.[69] A three-phased pilot training program was established under the ISE-SAR EE. Several stakeholders in the NSI—including the Office of the PM-ISE, DOJ, FBI, DHS, the International Association of Chiefs of Police (IACP), Major Cities Chiefs Association, Major County Sheriffs' Association, and National Sheriffs' Association—contributed to designing the curriculum. In addition, members of the privacy and civil liberties advocacy community reviewed and provided input about the training.

The first phase was the executive-level training for chiefs of police and their direct reports. It covered the SAR process, privacy and civil liberties issues, and the role chiefs and their staffs are expected to play in that process. IACP developed the second-phase training for front-line officers to recognize what type of activity might have a terrorist nexus and should be reported. It also covered privacy and civil liberties issues. An initial version was provided to 4,000 officers in the Washington, DC, area prior to the presidential inauguration. The third phase is for the intelligence analysts at fusion centers who will be responsible for vetting reports and making the final decision about entering SARs into the shared spaces environment.[70]

ISE-SAR EE Lessons Learned and the Way Ahead

The Office of the PM-ISE has conducted a preliminary review of lessons learned from the ISE-SAR EE. According to the pilot project participants:[71]

- There is clearly a value at the state, local, and tribal level from the implementation of a SAR process. This is based on the number of investigations

[68] See **Appendix A** for a description of the Guardian and *eGuardian* systems.

[69] Office of the PM-ISE briefing to CRS, July 20, 2009.

[70] Ibid.

[71] Office of the PM-ISE briefing to CRS, September 24, 2009.

initiated as a result of SAR reporting, referrals to the Joint Terrorism Task Forces (JTTF), and other leads.[72]

- It is possible to implement a SAR process that includes privacy and civil liberties protections.
- Delays in the incorporation of privacy and civil liberties issues into the SAR policy framework and training curriculum delayed the linkage of the various data repositories at the pilot sites. As a result, there is a shortage of quantitative data to validate the NSI concept. However, other output/outcome measures that will be used include the number of suspicious activity calls received; number of local SAR reports generated and vetted; number of SARs qualifying as ISE SARs and placed into the shared spaces, number of JTTF referrals and disposition of those referrals (new cases, existing cases); and number of non-JTTF criminal investigations, such as type of investigation and disposition (arrests, prosecutions, etc.).
- Although the ISE-SAR EE focused on the sharing of terrorism-related reports, it became apparent that the SAR process helped state and local governments with their risk assessments, the training of their law enforcement officers, and for the development of a common process for documenting and placing SARS in an accessible location. This suggested to the project team that the process will be of value in an "all crimes" context in addition to a counterterrorism one.

The Office of the PM-ISE intends to complete a full evaluation of the ISE-SAR EE and report to the Office of Management and Budget (OMB) by the end of 2009, with the results of the pilot project, recommendations about whether and how to implement the NSI program nationwide, and the establishment of an executive agent for SAR and an NSI program management office.[73]

The Freedom and Justice Foundation,[74] which has provided advice to the Office of the PM-ISE on the NSI project, also intends to produce a report about the NSI by year's end.[75] Among the recommendations it intends to make are the following:

- There should be a strong NSI program management office that will harmonize the various SAR activities of DOJ and DHS.
- The future NSI program management office should establish an audit function that can identify participant organizations who are not complying with the ISE Functional Standard or other NSI policies and direct training resources to those organizations.

[72] For example, between March 5, 2008, and October 20, 2009, in Los Angeles alone, 2,063 SARs were generated; 26 of these were relevant to open terrorism investigations; 151 of these were accepted by the JTTF for follow up; and 47 arrests were made (not necessarily terrorism-related crimes). Source: Briefing to CRS by Joan McNamara, Assistant Commander LAPD Counter-Terrorism and Criminal Intelligence Bureau, October 27, 2009.

[73] Office of the PM-ISE briefing for CRS, July 27, 2009, that references a PM-ISE Memorandum to the OMB Deputy Director for Management, "2008 Information Sharing Environment (ISE) Program Review Findings and Recommendations," October 28, 2008.

[74] On its website, the Freedom and Justice Foundation describes itself as "an educational non-profit working to enhance Centrist Public Policy development and implementation through the civic and interfaith engagement of Texas Muslims," at http://www.freeandjust.org/.

[75] Briefing to CRS by Mohamed Elibiary, President and CEO of The Freedom and Justice Foundation, October 12, 2009.

- Federal grant funding for fusion centers should be contingent upon compliance with the ISE's privacy and civil liberties policies. A fair process should be established for evaluating compliance with those policies and permit the suspension of grant funding for persistent non-compliance.

Current Administration Actions

In its FY2011 Programmatic Guidance for the ISE, the Administration also directed that Suspicious Activity Reporting be one of three ISE investment priorities that should be included in department and agency annual budget submissions to OMB.[76] It also directed departments and agencies to:

- Continue implementation and integration activities to institutionalize the NSI.
- As part of efforts to establish the ISE, DOJ and DHS will support the development of recommendations for Deputies (Deputy Secretaries of Cabinet Departments) regarding the establishment and functions of an interagency SAR Program Management Office that will oversee the NSI. [77]

Issues for Congress

In its forthcoming report to OMB, the PM-ISE is to make recommendations about whether and how to roll out the NSI on a nationwide basis. Congress may be interested in the following issues regarding program implementation.

Too Many "Dots"

The NSI is designed to increase the amount of information—the intelligence "dots"—that will flow from state, local, and tribal law enforcement agencies to the federal government. The goal of "connecting the dots" becomes more difficult when there is an increasingly large volume of "dots" to sift through and analyze. Because the NSI would establish mechanisms for—and indeed promote—the widespread reporting and sharing of data by numerous federal, state, and local agencies, some have expressed concerns about the risk of "'pipe clogging' as huge amounts of information are ... gathered without apparent focus."[78]

In an October 2007 report,[79] the Government Accountability Office (GAO) identified a related challenge. When "identical or similar types of information are collected by or submitted to multiple agencies, integrating or sharing this information can lead to redundancies." The GAO found "that in intelligence fusion centers, multiple information systems created redundancies of

[76] John O. Brennan; Jeffrey D. Zients, Deputy Director for Management, OMB; and Vivek Kundra, Federal Chief Information Officer; Memorandum to Cabinet Deputies, "FY 2011 Programmatic Guidance for ISE," July 28, 2009.

[77] Ibid., Tab A.

[78] Nojeim Testimony, March 18, 2009.

[79] GAO, Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers, GAO-08-35, October 30, 2007.

information that made it difficult to discern what was relevant. As a result, end users were overwhelmed with duplicative information from multiple sources."[80]

A challenge for the NSI is the extent to which the program will result in an avalanche of largely irrelevant or duplicative data while diverting the police from more productive law enforcement activities. For example, in a 40-month period before the ISE-SAR EE pilot program, the FBI documented approximately 108,000 potential terrorism-related threats, reports of suspicious incidents, and terrorist watchlist encounters.[81] The FBI expects the numbers to continue to grow.[82]

Congress may be interested in how a future SAR Program Management Office intends to address this problem—specifically, which agency or agencies will be responsible for quality control of SARs to prevent system overload from irrelevant or redundant ones and to ensure that the SARs that are entered into the shared space environment adhere to privacy and civil liberties standards.

Training

A national training program to educate law enforcement officers could enable law enforcement officers to place observed or reported behaviors into context in order to maximize the efficacy of efforts to discover possible criminal activity. It could also minimize the likelihood that they will document circumstances involving individuals who are actually involved in innocent and/or constitutionally protected activities.[83]

In addition, analysts at state and local fusion centers require training to perform their critical role of fusing intelligence and related information about suspicious activities in order to produce actionable intelligence. Numerous public, private, federal, state, and local databases can provide them with valuable information. The analysts typically need access to these data repositories and training in their use. Analysts also require training in the review of SARs that will enable them to identify duplicative information, distinguish the relevant from the irrelevant, and to make appropriate decisions about which reports should be entered into the ISE shared spaces environment.

Congress may wish to consider ways to provide funding to ensure that a comprehensive training program is part of any nationwide implementation of the NSI.

Data Privacy and Access

To achieve information-sharing objectives, government agency partners need to establish wide-scale electronic trust between the caretakers of sensitive information and those who need and are

[80] GAO, Interagency Collaboration: Key Issues for Congressional Oversight of National Security Strategies, Organizations, Workforce, and Information Sharing, GAO-09-904SP, September 2009, p. 50.

[81] Data was for the period July 2004 through November 2007. See DOJ, Office of the Inspector General Audit Division, *The FBI's Terrorist Threat and Suspicious Incident Tracking System*, Audit Report 09-02, November 2008, p. ii.

[82] Ibid.

[83] Initial Privacy and Civil Liberties Analysis of the ISE-SAR Functional Standard, September 2008, pp. 30-31.

authorized to use that information.[84] In its most recent publication, the Markle Task Force on National Security in the Information Age, maintains that

> [i]n an effective information sharing framework, information is not simply shared without restraint ... information sharing will succeed only if accompanied by government-wide policy guidelines and oversight to provide robust protections for privacy and civil liberties ... [i]ts governance should require a user to provide a predicate in order to access data under an authorized use standard. To establish a predicate, an analyst seeking information would need to state a mission- or threat-based need to access the information for a particular purpose."[85]

To accomplish this, proponents say that fusion centers must acquire a federated capability for identity and privilege management that securely communicates a user's roles, rights, and privileges to ensure network security and privacy protections. The two elements of this are identification/authentication—the identity of end users and how they were authenticated—and privilege management—the certifications, clearances, job functions, and organizational affiliations associated with end users that serve as the basis for authorization decisions.[86]

In order to protect sensitive data and the privacy of Americans, Congress may wish to examine the NSI policies that will govern data privacy and access to data within the ISE Shared Spaces environment. One question is whether to require and fund an auditor position within the future program management office to ensure compliance.

Information Technology (IT) Infrastructure

The success of the NSI is dependent on an IT infrastructure that enables state and local fusion centers to have access to each other's information as well as to the appropriate federal databases. Under the "shared space architecture" concept, fusion centers replicate data from their systems to an external server under their control. A secure portal is then created that allows simultaneous searching of all such databases so that fusion centers will be able to aggregate any relevant information that exists throughout the network. To connect into the system, a fusion center requires a server and software to translate data from whatever case management or intelligence system it uses to a separate database on the server.

Expenses for this IT infrastructure may exceed the funds that states and cities will allocate for their fusion centers from the State Homeland Security Grant Program (SHSGP) or Urban Area Security Initiative (UASI).[87] Congress may wish to consider ways to provide funding to fusion centers for this purpose.

[84] Briefing to CRS by Thomas O'Reilly, DOJ Bureau of Justice Assistance, June 15, 2009.

[85] Markle Task Force on National Security in the Information Age, *Nation at Risk: Policy Makers Need Better Information to Protect the Country*, March 2009, p. 7.

[86] For details on the Global Federated Identity Management framework which provides a standards-based approach for implementing federated identity, see DOJ, Office of Justice Programs, Justice Information Sharing, "Security and Federated Identity Management" at http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1179.

[87] For additional information about the use of SHSGP and UASI funds for homeland security, see CRS Report R40246, *Department of Homeland Security Assistance to States and Localities: A Summary and Issues for the 111th Congress*, by Shawn Reese.

Metrics

One of the biggest challenges facing policy makers is how to determine whether the NSI program is successful:

- Are the number of SARs produced or the number of SARs shared relevant metrics?
- How does one know if the SARs that are produced and shared under the program are actually meaningful intelligence "dots?"
- How does one determine if the right "dots" are being connected?

Congress may wish to ask how a future SAR Program Management Office would establish metrics to measure the success of an NSI program.

Appendix A. Significant Information-Sharing Systems

Law Enforcement Online (LEO)

Established prior to the 9/11 attacks, LEO is a secure, Internet-based communications portal for law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Managed by the FBI's Criminal Justice Information Services Division, LEO catalyzes and strengthens collaboration and information-sharing by providing access to sensitive but unclassified information and various state-of-the-art communications services and tools. It is available around the clock and is offered free of charge to members of the criminal justice and intelligence communities, as well as military and government agencies associated with infrastructure protection in the United States.[88]

Regional Information Sharing Systems Program (RISS)

Also established prior to the 9/11 attacks, RISS is a national network of six multistate centers designed to operate on a regional basis. It is federally funded and administered by DOJ's Bureau of Justice Assistance (BJA). RISS supports law enforcement efforts nationwide to combat illegal drug trafficking, identity theft, human trafficking, violent crime, and terrorist activity, and to promote officer safety. The regional centers provide member law enforcement agencies with a broad range of intelligence exchange and related investigative support services. RISS operates a secure intranet, known as RISSNet, to facilitate law enforcement communications and information sharing nationwide.[89]

Homeland Security Information Network (HSIN)

After the 9/11 attacks, DHS established the HSIN, a secured, Web-based platform for sensitive but unclassified information sharing and collaboration between federal, state, local, tribal, private sector, and international partners. The HSIN platform was created to interface with existing information-sharing networks to support the diverse communities of interest engaged in preventing, protecting from, responding to, and recovering from all threats, hazards, and incidents under the jurisdiction of DHS. There are five community of interest portals on HSIN: Emergency Management, Critical Sectors, Law Enforcement, Multi-Mission Agencies, and Intelligence and Analysis. HSIN provides real-time, interactive connectivity between states and major urban areas and the 24/7 DHS operations center—the National Operations Center (NOC).[90]

The HSIN-Intelligence portal provides state, local, and tribal officials with access to unclassified intelligence products. Classified intelligence products are provided to state and local fusion centers that have the appropriate security infrastructure through the Homeland Security Data Network (HSDN). Through HSDN, users can access collateral Secret-level terrorism-related

[88] See FBI, "Law Enforcement Online" at http://www.fbi.gov/hq/cjisd/leo.htm.

[89] See DOJ, Office of Justice Programs, Bureau of Justice Assistance, "RISS Program Brief." http://www.riss.net/overview.aspx.

[90] See DHS, *HSIN*, February 10, 2009, at http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm.

information including products from the National Counterterrorism Center's (NCTC) *NCTC Online*.

Law Enforcement Information Sharing Program (LEISP)

After 9/11, DOJ initiated the LEISP to foster the sharing of information across jurisdictional boundaries to prevent terrorism and to systematically improve the investigation and prosecution of criminal activity.[91] Two significant systems under the LEISP are described below:[92]

OneDOJ System

This system is a repository of data from DOJ law enforcement components (Bureau of Alcohol, Tobacco, Firearms, and Explosives; Bureau of Prisons; Drug Enforcement Administration; FBI; and the U.S. Marshals Service) that enables the sharing of investigative information within the department. It is hosted at the FBI's Criminal Justice Information Services (CJIS) data center. External sharing is accomplished through bilateral partnerships with designated regional, state, or federal sharing initiatives. These partnerships allow non-DOJ users to access OneDOJ data from within their own systems and vice-versa. However, data are not contributed by external partners to the OneDOJ system.

Law Enforcement National Data Exchange (N-DEx)

N-DEx is intended to facilitate the sharing of information across jurisdictional boundaries and to provide new investigative tools that enhance the nation's ability to fight crime and terrorism. Its proposed services and capabilities would allow participating agencies to detect relationships between people, places, things, and crime characteristics; to link information across jurisdictions; and to "connect the dots" between apparently unrelated data without causing information overload.

FBI Terrorist Tracking Systems

After 9/11, the FBI established two programs for the tracking, analysis, and sharing of information about terrorism threats:

Guardian

Guardian is described as a classified information technology system that allows the FBI to collect and review reports of suspicious activity in an organized way to determine which ones warrant additional investigative follow-up.[93] The primary purpose is not to manage cases, but to facilitate the reporting, tracking, and management of threats to determine within a short time span whether a particular matter should be closed or referred for an investigation. Guardian's database can be

[91] DOJ, "Law Enforcement Information Sharing Program (LEISP)," at http://www.usdoj.gov/jmd/ocio/leisp/.

[92] DOJ, "LEISP Initiatives," at http://www.usdoj.gov/jmd/ocio/leisp/initiatives.htm.

[93] FBI, "*eGuardian* Threat Tracking System," http://foia.fbi.gov/eguardian_threat.htm. Hereafter: "FBI, *eGuardian* Threat Tracking System."

searched by FBI employees and certain other government agency partners thus providing a capability to analyze threat information for trends and patterns.[94]

eGuardian

A companion system to Guardian is *eGuardian*. It is an unclassified system designed to enable near real-time sharing and tracking of terrorist information and suspicious activity with federal, state, local, and tribal agencies.[95] Unclassified information from the Guardian system that appears to have a potential nexus to terrorism is to be passed down to *eGuardian*, where it will be available for viewing by those members of state, local, and tribal law enforcement and representatives of other federal law enforcement agencies that have been given permission to access the system.[96] It is also intended to serve as the mechanism for the electronic transmittal of leads by state, local, and tribal agencies to the JTTF's. FBI has made *eGuardian* available on its secure LEO Internet portal, allowing more than 18,000 agencies to run searches and input their own reports.

[94] DOJ, Office of the Inspector General Audit Division, *The FBI's Terrorist Threat and Suspicious Incident Tracking System,* Audit Report 09-02, November 2008, p. 1.

[95] FBI, "Connecting the Dots: Using New FBI Technology," September 19, 2008, at http://www.fbi.gov/page2/sept08/eguardian_091908.html.

[96] FBI, "*eGuardian* Threat Tracking System."

Appendix B. Acronyms Used in This Report

ACLU	American Civil Liberties Union
BJA	Department of Justice, Bureau of Justice Assistance
CAPPS II	Computer Assisted Passenger Prescreening System II
CCAD	Consolidated Crime and Analysis Database
CDT	Center for Democracy and Technology
DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
GLOBAL	Global Justice Information Sharing Initiative
HSIN	Homeland Security Information Network
IACP	International Association of Chiefs of Police
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
IT	Information Technology
ISE	Information Sharing Environment
ISE SAR	Information Sharing Environment Suspicious Activity Report
ISE-SAR EE	Information Sharing Environment Suspicious Activity Report Evaluation Environment
JRSA	Joint Research and Statistics Association
JTTF	Joint Terrorism Task Force
LAPD	Los Angeles Police Department
LEOe	Law Enforcement Onlin
N-DEx	Law Enforcement National Data Exchange
NSAC	FBI National Security Analysis Center
NSI	Nationwide Suspicious Activity Report Initiative
ODNI	Office of the Director for National Intelligence
OMB	Office of Management and Budget
PM-ISE	Program Manager for the Information Sharing Environment
RISS	Regional Information Sharing Systems Program
SAR	Suspicious Activity Report
SHSGP	State Homeland Security Grant Program
TIA	Total Information Awareness Program
UASI	Urban Area Security Initiative

Author Contact Information

Mark A. Randol
Specialist in Domestic Intelligence and Counter-Terrorism
mrandol@crs.loc.gov, 7-2393