Available online at www.sciencedirect.com

SCIENCE DIRECT®

Government Information Quarterly 21 (2004) 420–438

Government Information Quarterly

Homeland security and information sharing: Federal policy considerations ☆

Harold C. Relyea*

Congressional Research Service, Library of Congress, Washington, DC 20540-7470, USA

Abstract

Inadequate information sharing by federal entities was a factor in the terrorist attacks of September 11, 2001. Among the responses to this shortcoming is Section 892 of the Homeland Security Act of 2002, which mandates the prescription of homeland security information-sharing procedures by the President. This responsibility has been delegated to the Secretary of Homeland Security, and the required procedures are expected to be issued in some form, preliminary or final, during the summer of 2004. Those developing these procedures will encounter what one information security expert describes as "a series of bureaucratic fiefdoms, a veritable 'patchwork quilt,' that has come about as a consequence of a hodgepodge of laws, regulations and directives with respect to how the Federal Government handles and discloses information." Examined in this review are some of the discernable uncertainties in the creation of the information-sharing procedures, and some of the policy considerations involved.
Published by Elsevier Inc.

1. Introduction

"Homeland security," as noted previously in this journal, came into public parlance in the aftermath of the September 2001 terrorist attacks on the World Trade Center and the Pentagon, evolved into a policy concept, and has come to be seen, during the course of that

☆ The views expressed in this article are those of the author and do not necessarily reflect the position of the Library of Congress or the Congressional Research Service.

* Fax: +1 202 707 3325.

E-mail address: hrelyea@crs.loc.gov.

0740-624X/$ - see front matter. Published by Elsevier Inc.
doi:10.1016/j.giq.2004.08.007

evolution, to have some historical foundation, civil defense being a primary antecedent.[1] The *National Strategy for Homeland Security*, issued by President George W. Bush on July 16, 2002, defined "homeland security" as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[2] The national strategy served by this concept of homeland security clearly recognizes the critical importance of information sharing for its realization, as well as the need to balance homeland security requirements with countervailing values, such as personal privacy.[3]

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."[4] Prior to so defining homeland security information as used in the section, 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 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.[5] Neither the 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 that "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 the referred to 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 referred to 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 [FBI]." 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 and local information, it is to 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.[6]

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, nondisclosure 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.[7]

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.

Other sections of the information-sharing subtitle authorize the sharing of grand jury, communications intercept, foreign intelligence, electronic surveillance, and physical search information. While these provisions seemingly have some bearing upon "homeland security,"

the focus of this analysis is upon the policy considerations arising from Section 892. Is existing policy adequate for all aspects of the comprehensive information-sharing program anticipated in Section 892? The answers to that question will be easier to provide once the details of the President's procedures are made known (if, indeed, they are publicly released). Until they are disclosed, the following overview provides some preliminary assessment of some of the policy considerations involved.

2. Pursuing new arrangements

Inadequate information sharing by federal entities—between field and headquarters offices and among law enforcement and intelligence agencies—was a factor in the terrorist attacks of September 11, 2001. In the House of Representatives, a legislative remedy was offered in early 2002, adopted in modified form in June, and attached in July as a floor amendment to legislation establishing a Department of Homeland Security (DHS). The provisions remained in the DHS chartering legislation signed into law by the President in November.[8] The following year, at a May hearing assessing barriers to information sharing in DHS, some members of the House Committee on Government Reform were lamenting the findings of a recent General Accounting Office (GAO) report concluding that, 20 months after the terrorists attacks and 6 months after the enactment of the Homeland Security Act, better integration and sharing of terrorist-related information—terrorist watch lists were the area of focus—were needed.[9] GAO examined nine federal agencies which have developed and maintain 12 watch lists, and found that while "the federal agencies that have watch lists share the lists among themselves," only "half of these agencies share their respective lists with state and local agencies, and one-fourth share them with private entities." The report noted that a principal barrier to improved sharing was technological in nature, saying: "The extent to which sharing is accomplished electronically is constrained by fundamental differences in watch list system architectures (that is, the hardware, software, network, and data characteristics of the systems).[10] Two of the nine agencies examined by GAO "reported that they did not have any policies and procedures on watch list sharing." GAO indicated that an "effective way to implement such policies and procedures [that define the rules governing sharing] is to prepare and execute written watch list exchange agreements or memorandums of understanding . . . [to] . . . specify answers to such questions as what data are to be shared with whom, and how and when they are to be shared." Of the seven agencies in the GAO study "that reported having such policies and procedure, one did not require any written agreements" for sharing. Moreover, "the policies and procedures of the seven have varied," said the report. In conclusion, GAO found that "federal agencies do not have a consistent and uniform approach to sharing watch list information."[11]

In his prepared statement for the House Committee on Government Reform, Steven I. Cooper, Chief Information Officer (CIO) for DHS, identified several information-sharing initiatives underway at the department. These included the March 2003 completion of "a policy and technical framework to promote information sharing among the Department of Justice, the Intelligence Community and the Department of Homeland Security . . . that provides a framework for implementing an integrated 'watch' list"; "the extension of law

enforcement information sharing networks such as the Regional Information Sharing Network (RISSNET) to provide a distribution channel for law enforcement homeland security information"; "working with 'best of the breed' regional information sharing groups such as the Emergency Response Network of Dallas, Texas (ERN), to provide homeland security information to a broad cross-section of first responders"; and "providing secure video conference capability to governors and emergency response centers for each of the 56 states, territories or protectorates."[12] In view of the fact that the department had been in operation only since January 24, these were good efforts, but they probably did not satisfy critics who felt that the Bush Administration, through the Office of Homeland Security, where Cooper had served before coming to DHS, should have initiated information-sharing improvements shortly after the July 2002 issuance of the *National Strategy for Homeland Security*, which identified several such areas for reform.[13]

In an August 2003 report to the Secretary of Homeland Security, GAO provided the results of a survey of officials "knowledgeable about information sharing from federal, state, and city agencies and officials from associations representing cities, police organizations, and research groups," which was conducted "before the Department of Homeland Security (DHS) began operations in January 2003." In addition, "to supplement this analysis," said the report, "we conducted a survey of officials representing the federal intelligence community and law enforcement agencies; state homeland security offices; all cities with a population of 100,000 or more; and a sample of cities with a population between 50,000 and 100,000, to obtain their perceptions about the current information-sharing process." It indicated that the "overall response rate for the survey was 50 percent and represents 284 government entities."[14]

The report acknowledged several information-sharing actions that had recently occurred, such as the active development of an enterprise architecture by DHS;[15] the February publication of the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, which called for improved information sharing;[16] and the issuance of the July presidential directive assigning responsibilities for developing the information-sharing procedures mandated by Section 892 of the Homeland Security Act.[17] Also identified were some information-sharing initiatives that had been discovered during the course of GAO's survey research. The FBI had "significantly increased the number of its Joint Terrorism Task Forces." California had "established an antiterrorism information center that collects, analyzes, and disseminates information to its law enforcement officers, other law enforcement agencies, and FBI." Moreover, said the report, "34 of 40 states and 160 of 228 cities stated that they participate in information-sharing centers." Assessing these developments, GAO offered a note of caution.

> While these initiatives may increase the sharing of information to fight terrorism, they are not well coordinated and consequently risk creating partnerships that may actually limit some participants' access to information and duplicating efforts of some key agencies in each level of government. Moreover, while beneficial to these participants, the initiatives do not necessarily integrate others in a truly national system and may inadvertently hamper information sharing for this reason. A lack of effective integration could increase the risk that officials will overlook, or never even receive, information needed to prevent a terrorist attack.[18]

Survey results generally revealed that existing information-sharing arrangements were largely not considered to be effective: "only 13 percent of federal government respondents

reported that sharing information with states and cities was 'effective' or 'very effective" . . . [and], of the 40 states that responded, only 35 percent reported that sharing with the federal government was 'effective' or 'very effective.'" Why? Three main systemic problems that accounted for this perception were identified: (1) "no level of government was satisfied that they receive enough information"; (2) "no level of government was satisfied with the timeliness, accuracy, or relevance of the information they received"; and (3) "the federal government still perceives the fight against terrorism, particularly its prevention, to be generally a federal responsibility, which potentially undermines the unity of effort between federal, state, and city governments needed to effectively secure the homeland. Consequently," noted the report, "the federal government still has not established comprehensive policies or procedures to effectively integrate state and city governments into the information-sharing process or even routinely recognize their role in this process." While federal agencies participating in the GAO survey "identified several barriers to sharing threat information with state and city governments," the participating "state and city governments did not perceive that the barriers identified by the federal agencies were truly barriers." For example, noted the report, "when federal agencies felt they could not provide states and cities with information, they cited concerns over state and local officials' ability to secure and protect classified information, the officials' lack of security clearances, and the lack of integrated databases." GAO indicated that these barriers could be overcome with proper training, new equipment, and building upon state and local experience with routinely handling and protecting "law enforcement sensitive" information in bringing cases against suspected criminals. The report recommended that "the Secretary of Homeland Security, in developing the enterprise architecture, (1) work in conjunction with the heads of other federal agencies, state and city authorities, and the private sector to ensure that the department's enterprise architecture fully integrates them into the information-sharing process and (2) take specific actions, including obtaining the private sector's views regarding information sharing, to evaluate and overcome the perceived barriers that prevent information sharing today."[19]

Appearing at about the same time as the GAO report was one prepared by the minority staff of the Senate Committee on Governmental Affairs, which reiterated some of the same concerns about the adequacy of intergovernmental information-sharing arrangements. Based upon interviews with state and local officials, as well as public information sources, the staff report found that these officials "do not systematically receive from the Bush Administration the information they need to prevent or respond to another catastrophic terrorist attack, nor does vital information flow effectively from them to the federal government." Moreover, what these officials "want most is to have a seat at the table as the administration grapples with homeland security protection. They need," said the report, "reliable and timely information about terrorist threats, individuals on federal terrorist watch lists, and investigations of suspected terrorists in their jurisdictions." Regarded to be "extremely troublesome" was the federal government's neglect of "the information needs of our nation's local fire fighters . . . because fire fighters nationwide are most communities' first line of defense against conventional, chemical, radiological, and biological attacks." Other difficulties identified were delays (and, perhaps, the cost) state and local officials experienced in receiving security clearances in order to have access to security classified information, and determining or

defining the "many different categories of information that is [sic] of varying interest to a host of different state and local officials."[20]

Among the recommendations made by the report to improve the information-sharing situation were as follows: make consolidated federal watch lists available to state and local government law enforcement agencies; utilize national and regional task forces to coordinate the information-sharing needs of the three levels of government, and provide state and local officials a permanent "seat at the table" regarding those needs; expedite security clearances for designated subnational government officials, and explore improving reciprocity among federal agencies regarding clearances; expedite the establishment of 24-hour operations centers in each state; require the performance evaluation of responsible senior federal managers regarding, in part, their success or failure in breaking down barriers to information sharing; and make sharing homeland security information with state and local officials a "high priority" for DHS and other key agencies.[21]

Concerning the President's responsibility, pursuant to Section 892 of the Homeland Security Act, to prescribe and implement information-sharing procedures, the report noted the "Bush Administration first issued an Executive Order delegating responsibility for prescribing the required procedures on July 29, 2003—9 months after the Act was passed, and 3 months before it is to report on its progress to the Congress."[22]

The Senate minority staff report was also critical about another administration innovation. The Homeland Security Act mandated the Information Analysis and Infrastructure Protection Directorate within DHS as "a central location to integrate, analyze, and disseminate intelligence information related to terrorist threats across all levels of government, especially including state and local governments," noted the report.[23] The directorate is responsible for, among other duties, coordinating "training and other support to the elements and other personnel of the Department, other agencies of the Federal Government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department."[24]

Instead of implementing the mandate of the directorate to function as an all-sources intelligence center within DHS, the Bush Administration administratively created, with some resulting controversy, a Terrorist Threat Integration Center (TTIC) outside of the department that reports to the Director of Central Intelligence.[25] The minority staff report quoted the criticism of Senator Joseph I. Lieberman. (D-CT), the ranking minority member of the Committee on Governmental Affairs, regarding this development: "The fundamental problem is that by placing the TTIC under the command of the Central Intelligence Agency [CIA] and not the Department of Homeland Security, it will be removed from our government's daily efforts to improve domestic defenses, constrained by cultural and institutional rivalries between the CIA and the FBI, isolated from state and local governments, and unaccountable to the nation's top homeland security official"—Secretary Tom Ridge. Noting that Secretary Ridge subsequently defended the administration's creation of TTIC, the report comments that "he failed to adequately address one of Senator Lieberman's key concerns: as constituted, the TTIC, under the Director of Central Intelligence, would not effectively incorporate state and local law enforcement into anti-terror intelligence activities."[26]

Public administration expert Donald F. Kettl of the La Follette School of Public Affairs at the University of Wisconsin-Madison echoed this criticism of TTIC in his assessment of DHS's first year of operations. In his view, "TTIC became a new arena in which the FBI and the CIA continued their ongoing scuffles over domestic and foreign intelligence." While he thought "TTIC has demonstrated progress in coordinating intelligence," Kettl considered DHS to have a "marginal role in the collection and analysis process," which "has hindered its ability to lead homeland security policy." He called for a clarification of the DHS relationship with TTIC, a clarification of the DHS intelligence role, development of a clear protocol for sharing intelligence information with state and local officials, and a clarification of the standards for collecting and retaining homeland security data.[27]

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.[28]

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.[29]

"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*.[30] 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 infrastructure of the United States," and specifies certain systems to be included in such plan.[31]

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."[32]

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 the following:

- member access to electronic information via email and Web sites;
- secure members-only access to information on the ISAC Web site;
- conference calls for members; and
- other IT such as pagers, telephone calls, and faxes to disseminate information.[33]

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.[34]

That same month, an issue paper prepared by the minority staff of the House Select Committee on Homeland Security for Representative Jim Turner (D-TX), the ranking minority member of the panel, indicated that "there are still numerous obstacles to effective information sharing in the federal government." Among the shortcomings identified in the paper were the lack of a fully integrated terrorist watch list; haphazard federal agency to agency sharing of threat information; ineffective information sharing with state and local governments; ineffective dissemination of information by the Terrorist Screening Center; an existing structure for intelligence information sharing that senior government officials have conceded to be unwieldy; "major weaknesses in how the Executive Branch defines the respective roles, responsibilities, and authorities of the Federal agencies involved in assessing and disseminating homeland security information"; and "poor interoperability between DHS and its Intelligence Community partners."[35]

DHS, it should be noted, has developed a communications capability, through the Joint Regional Information Exchange System (JRIES), between its Homeland Security Operations Center and, as of February 24, 2004, all 50 states, five territories, the District of Columbia, and 50 major urban areas. This secure system, part of the Homeland Security Information Network (HSIN), immediately delivers real-time threat information of a sensitive but unclassified character to all users and provides a basis for future security classified communications. Subnational participants include state National Guard offices, Emergency Operations Centers, and first responder and public safety entities.[36] In a related development, Sprint has created Peerless IP, a government grade Internet protocol-based intranet, impenetrable to outside cyber attacks. It is a realization of the GovNet proposal debated in the months after the September 2001 terrorist attacks. Demand is reportedly rising among federal agencies for connection with the new system, which is both physically and virtually private, providing an exclusively intergovernmental communication and information-sharing network.[37]

3. Framing the new procedures

Against this background, and in response to some of the issues noted, Secretary Ridge will develop and provide to the President, for his approval and implementation, the homeland security information-sharing procedures mandated by Section 892 of the Homeland Security Act. Others, in accordance with E.O. 13311, will be making input, as well, including the Attorney General, the Director of Central Intelligence, and specified officials with whom Secretary Ridge is to coordinate. How that set of procedures will be formulated has not been made publicly known by DHS. Will state and local government officials, for example, be provided the "seat at the table" that the recent GAO and Senate Governmental Affairs minority staff reports recommended, or will their input, and that of other interests, be accommodated by a rumored public comment opportunity when the

draft procedures emerge in the summer sun? Preparatory to viewing those procedures, whether in draft or final form, what are some of the policy considerations arising from Section 892?

3.1. Custody

An initial consideration concerns the "ownership" or custody of shared information. For the 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." This language allows federal agencies to remove their information from the sharing system, and to demand its withdrawal from state and local government data banks. 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. Leaving aside the matter of readily identifying the state or local government origin of information so shared with federal agencies, 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."[38] 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? "

Prior to the 1989 *Tax Analysts* decision of the Supreme Court, lower courts, in determining whether an agency had sufficient control over materials, had examined the purpose for which the materials had been obtained by a federal agency.[39] In the aftermath of the *Tax Analysts* ruling, federal courts continued this practice, with the result that they began to extend the scope of the FOIA to include records in the possession of a government contractor.[40] Thus, it seems likely that, should a court be 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 rule that such information is subject to FOIA access, is the matter of the applicability of the statute's nine exemptions to the rule of disclosure and other provisions protecting law enforcement information.[41]

3.2. Protection

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 [from its protected status], 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." In the next subsection, the President is directed, when prescribing the mandated information-sharing procedures, "to protect the constitutional and statutory rights of any individuals who are subjects of such information."[42] Among the types of protected information so identified are those which are "sensitive but unclassified," are classified, and 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" are referenced by the Homeland Security Act regarding "sensitive but unclassified" information.[43] 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.[44]

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."[45] What constitutes "sensitive" information for this section is not evident as 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 to be 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.[46]

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 US$4 million expansion of the Upstate New York Regional Intelligence Center, jointly operated by New York State and the FBI. It was 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.[47] 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 as 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."[48] 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.[49] 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 Director of Central Intelligence.[50] 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 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.[51] Operative security classification policy does not authorize the classification of this information, which remains the private property of the submitter.[52]

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."[53] A more detailed explanation of SSI may be found in the regulations.[54] 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 impliedly 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.[55]

Speaking at the summer meeting of the National Governors Association last year, 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.[56] Presumably, the states paid for the background investigations for these clearances, each costing upwards of US$2500 or more, 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.

3.3. Quality

Finally, Section 892 begs 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.

4. Overview

When legislating the Homeland Security Act, Congress recognized the importance of effective information sharing among government jurisdictions and selected private entities to combat terrorism and secure the homeland. Included in that statute is the Homeland Security Information Sharing Act, which mandates the President to prescribe procedures facilitating homeland security information sharing. Acting on behalf of the President in this regard, Secretary Ridge will confront what J. William Leonard, director of the Information Security Oversight Office, described not long ago as "a series of bureaucratic fiefdoms, a veritable 'patchwork quilt,' that has come about as a consequence of a hodgepodge of laws, regulations and directives with respect to how the Federal Government handles and discloses information."[57] Some of the authorities he referred to have been identified and discussed here. Congress, also aware of this array of policies, elected to refer to what they control in such broad terms as "security classified" and "sensitive but unclassified" information. Disappointed with this course, Mr. Leonard expressed his firm belief "that never before have we had such a clear and demonstrable need for a seamless process for sharing and protecting information, regardless of classification." Nonetheless, he feared, "in many ways, we are not only continuing the current 'patchwork quilt,' but we are quite possibly adding new seams every day," with the result that "these seams not only can serve as impediments to information sharing, they can also develop into the tears in the fabric through which information that requires protection may slip, as well intentioned individuals use work-around procedures in order to get the job done."

Perhaps the better course, for Mr. Leonard and for legislators, might have been to direct the President not to prescribe homeland security information-sharing procedures administratively, but to provide Congress with a plan for realizing information-sharing arrangements legislatively. Upon receiving this plan, Congress, in Mr. Leonard's words, would "take the initiative and begin the process to develop and implement a seamless and congruous system for protecting and sharing all types of information, both classified and unclassified." This approach also would have kept policy determination for this matter within the congressional domain. That Section 892 of the Homeland Security Act mandates presidential prescription of homeland security information-sharing procedures does not mean, however, that the opportunity sought by Mr. Leonard to realize "a seamless and congruous system for protecting and sharing all types of information" has been lost forever. After the President's procedures have been implemented, their efficiency and effectiveness will be subject to congressional evaluation. To the extent that these procedures are found to be in need of improvement, Section 892 may be amended to bring about the desired reform.

Notes and references

1. See Relyea, Harold C. (2002). Homeland security and information. *Government Information Quarterly, 19,* 213–223.
2. U.S. Office of Homeland Security. (2002, July). *National strategy for homeland security* (p. 2). Washington: GPO.
3. See Ibid., pp. 55–58.
4. 116 Stat. 2255.
5. 116 Stat. 2253 (emphasis added).
6. 116 Stat. 2254.
7. 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.
8. The initial bill, H.R. 3825, was introduced on February 28, 2002, by Representative Saxby Chambliss (R-GA) for himself and 28 bipartisan cosponsors. A modified version, H.R. 4598, with 33 bipartisan cosponsors, was adopted by the House on June 26, and a version of it was appended to H.R. 5005, chartering a Department of Homeland Security, on July 25 during floor debate, and remained in the enacted law. See Congressional Record, 148 (July 25, 2002): H5854–H5861 (daily edition); 116 Stat. 2135 at 2252.
9. U.S. Congress, House Committee on Government Reform. (2003, May 8). *Out of many, one: Assessing barriers to information sharing in the Department of Homeland Security. 108th Congress, 1st session, hearing* (pp. 7–14). Washington: GPO.
10. U.S. General Accounting Office. (2003, April). *Information technology: Terrorist watch lists should be consolidated to promote better integration and sharing* (GAO Report GAO-03-322, p. 2). Washington.
11. Ibid., p. 17.
12. U.S. Congress, House Committee on Government Reform. *Out of many, one: Assessing barriers to information sharing in the Department of Homeland Security*, p. 21.
13. See U.S. Office of Homeland Security, *National strategy for homeland security*, pp. 55–58.
14. U.S. General Accounting Office. (2003, August). *Homeland security: Efforts to improve information sharing need to be strengthened* (GAO Report GAO-03-760, pp. 1–2) Washington.
15. According to the report, "An enterprise architecture can be viewed as a blueprint that describes an entity's operational and technical environments. The blueprint," it continued, "includes descriptive models of the entity's current and future business and technical environments, along with a roadmap for transitioning from the current to the future environment." Ibid., p. 2n.
16. U.S. White House Office. (2003, February). *The national strategy for the physical protection of critical infrastructures and key assets* (pp. 25–27). Washington: GPO.
17. E.O. 13311 in Federal Register. (2003, July 31). Vol. 68, pp. 45149–45150.
18. U.S. General Accounting Office. *Homeland security: Efforts to improve information sharing need to be strengthened*, p. 4.

19. Ibid., pp. 4–6.
20. U.S. Congress, Senate Committee on Governmental Affairs. (2003). *State and local officials: Still kept in the dark about homeland security* (report prepared by the minority staff). *108th Congress, 1st session, committee print* (pp. 1–2). Washington: GPO.
21. Ibid., pp. 2–4, 20–24.
22. Ibid., pp. 8–9; Section 893 of the Homeland Security Act requires the President, not later than 12 months after the date of the enactment of the statute, which was November 25, 2002, to submit a report to the House and Senate Judiciary and Intelligence committees on the implementation of Section 892.
23. U.S. Congress, Senate Committee on Governmental Affairs. *State and Local Officials: Still kept in the dark about homeland security*, p. 9; see 116 Stat. 2145.
24. 116 Stat. 2148.
25. See U.S. Congress. House Committee on the Judiciary and Select Committee on Homeland Security. (2004). *Terrorist Threat Integration Center (TTIC) and its relationship with the Departments of Justice and Homeland Security. 108th Congress, 1st session, joint hearing, July 22, 2003*. Washington: GPO.
26. U.S. Congress, Senate Committee on Governmental Affairs. *State and local officials: Still kept in the dark about homeland security*, pp. 9–10.
27. Kettl, Donald F. (2004, March 4). *The Department of Homeland Security's First Year: A report card* (uncorrected manuscript, pp. 20–21). Century Foundation. Available: http://www.tcf.org/Publications/HomelandSecurity/ovewview.pdf
28. U.S. General Accounting Office. (2003, September 17). *Homeland security: Information sharing responsibilities, challenges, and key management issues* (GAO Testimony GAO-03-1165T, pp. 2–3). Washington.
29. Ibid., pp. 12–15.
30. See U.S. Office of Homeland Security. *National strategy for homeland security*, p. 33.
31. U.S. White House Office. (2002, November 25). *Department of Homeland Security Reorganization Plan* (p. 9). Washington.
32. U.S. General Accounting Office. (2004, April 21). *Critical infrastructure protection: Establishing effective information sharing with infrastructure sectors* (GAO Testimony GAO-04-699T, p. 2). Washington.
33. 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.
34. Ibid., pp. 23, 24–26.
35. House Select Committee on Homeland Security. (2004, April). *Information sharing for homeland security: Obstacles to effective information sharing still exist post 9/11* (Issue Paper 1, pp. 2–5).
36. U.S. Department of Homeland Security. (press release, 2004, February 24). *Homeland security launches expansion of information exchange system to states and major cities*. Available: http://www.dhs.gov/dhspublic/display?theme=43&content=3212&print=true; U.S. Department of Homeland Security. (press release, 2004, February 24). *Homeland Security Information Network to expand collaboration, connectivity for states and major*

cities. Available: http://www.dhs.gov/dhspublic/display?theme=43&content=3350&print=true
37. New, William. (2004, January 29). Demand grows for government-only computer network. *GovExec.com* (daily briefing). Available: http://www.govexec.com/dailyfed/0104/012904tdpm1.htm
38. *DOJ v. Tax Analysts*, 492 U.S. 136, 144–145 (1989).
39. See *Ryan v. DOJ*, 617 F.2d 781 (D.C. Cir 1980); *St. Paul's Benev. Ed. & Miss. Inst. v. U.S.*, 506 F. Supp. 822 (N.D.Ga. 1980); *RCA Global v. FCC*, 524 F. Supp. 579 (D. Del. 1981); *International Brotherhood of Teamsters v. National Mediation Board*, 111 L.R.R.M. (BNA) 2020 (D.D.C. 1982, affirmed, 712 F.2d 1495 (D.C. Cir. 1983); *General Electric Co. v. NRC*, 750 F.2d 1394 (7th Cir. 1984); *Hercules, Inc. v. Marsh*, 839 F.2d 1027 (4th Cir. 1988).
40. See *Burka v. HHS*, 87 F.3d 508 (D.C. Cir. 1996); *Los Alamos Study Group v. DOE*, No. 97-1412 (D. N.M. July 22, 1998); *Chicago Tribune Co. v. HHS*, 1999 WL 299875 (N.D. Ill. May 4, 1999). These ruling have been made notwithstanding the holding of the Supreme Court in *Forsham v. Harris*, 445 U.S. 169 (1980).
41. See 5 U.S.C. 552(b)–(c).
42. 116 Stat. 2253–2254.
43. See 101 Stat. 1724; 15 U.S.C. 278g–3.
44. 101 Stat. 1730; 40 U.S.C. 759 note, subsequently repealed 1996, 110 Stat. 680.
45. 116 Stat. 2922.
46. U.S. Department of Homeland Security, Management Directive System. (2004, May 11). *Safeguarding sensitive but unclassified (for official use only) information* (MD Number 11042).
47. Johnston, David. (2004, May 25). *Terror data to be shared at New Center near Albany* (p. A20). New York Times.
48. 5 U.S.C. 551(b)(1).
49. 3 C.F.R., 1995 Comp., pp. 333–356; 3 C.F.R., 2003 Comp., pp. 196–218.
50. See 42 U.S.C. 2014(y); 50 U.S.C. 403–3(c)(6).
51. See 116 Stat. 2150–2155.
52. 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 1 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).
53. See 49 U.S.C. 114(s), 40119; this general definition of SSI appears in *Federal Register* (2002, February 22). Vol. 67, p. 8342.
54. See 49 C.F.R. 1520.7.
55. See *Public Citizen, Inc. v. FAA*, 988 F.2d 186 (D.C. Cir. 1993).
56. Janofsky, Michael (2003, August 19). Intelligence to be shared, Ridge tells governors.

New York Times, A17; the prepared text of Secretary Ridge's remarks is available at http://www.dhs.gov/dhspublic/display?theme=44&content=1200&print=true

57. "Information sharing and protection: A seamless framework or patchwork quilt?" remarks of J. William Leonard, Director, Information Security Oversight Office, at the National Classification Management Society's (NCMS) Annual Training Seminar, Salt Lake City, UT, June 12, 2003, available at http://www.fas.org/sgp/isoo/ncms061203.html