23

INFORMATION SHARING WITH THE PRIVATE SECTOR

History, Challenges, Innovation, and Prospects

Daniel B. Prieto

The terrorist attacks of September 11, 2001, fundamentally challenged two key aspects of U.S. national security thinking. First, it altered the relationship between the private sector and the federal government by squarely thrusting the private sector into a new and unprecedented national security role. Second, it challenged long-standing priorities regarding the treatment of national security information, increasing the importance of sharing information and making it more widely available at the expense of traditional limitations on access to and dissemination of classified and other sensitive information.

This chapter addresses the confluence of these challenges – information sharing by the federal government with the private sector to enhance national and homeland security. It provides a brief history of public–private information sharing efforts before 9/11, describes reforms and initiatives since 9/11, and assesses problems and prospects for improved information sharing in the future.

THE NEW NATIONAL SECURITY ROLE OF THE PRIVATE SECTOR

The use of commercial aircraft as missiles against the World Trade Center and the Pentagon, and subsequent Al Qaeda statements declaring its intention to "fill [American] hearts with terror and target [America's] economic lifeline,"[1] made it clear that private sector facilities – including transportation, energy, water, chemicals, telecommunications, computers, and the food supply – are attractive terrorist targets. More than 85 percent of the hundreds of thousands of critical infrastructure facilities in the United States are owned by the private sector. The federal government has acknowledged the private sector as a critical

partner in homeland security in strategy, policy, and in the homeland security reorganization efforts of the federal government since 9/11.

The critical homeland security role of the private sector was again made clear in late 2005. Hurricane Katrina devastated New Orleans and other coastal areas in Louisiana, Mississippi, and Alabama, becoming the most destructive and costly natural disaster in the history of the United States, and one of the deadliest. The official death toll neared 1,400, an additional 1,300 were missing and "feared dead," damages were estimated between $100 billion and $200 billion, and more than a million people were displaced. The private sector played a key role in providing an effective response to Hurricane Katrina. In some areas, Wal-Mart, Target, and Home Depot provided manpower, materials, and logistics to become key distribution points for food, water, clothing, generators, and other supplies. Mississippi Power, a subsidiary of Southern Company, restored electricity to hundreds of thousands of customers well ahead of schedule. Starwood Hotels provided vital services to its customers, employees, and first responders during and immediately after the storm.

Hurricane Katrina illustrated the need for better integration of the private sector into America's security equation. For this to happen, information sharing between the federal government and the private sector needs to improve and be supported by more clearly understood roles and responsibilities, well-developed trust relationships, and clear protocols and mechanisms for sharing. While progress has been made since 9/11, more needs to be done.[2]

The 9/11 attacks demonstrated the ability and willingness of terrorists to target U.S. economic infrastructure and use it as a weapon against civilians. Katrina illustrated that the private sector brings resources and logistical capabilities that are a necessary complement to federal, state, and local homeland security capabilities. The private sector is now a critical front-line national security player that will be essential to detect, prevent, and respond to future terrorist threats.

POLICY AND INITIATIVES BEFORE 9/11

Spurred by the rapid growth in the use of information technology in the mid-1990s, President Clinton created the President's Commission on Critical Infrastructure Protection. The commission addressed vulnerabilities in key sectors in the U.S. economy generated by an increased reliance on and interconnectivity resulting from the expanded use of information technology. In 1997, the commission called for a national effort to address the growing vulnerability of these critical infrastructures on which the nation's health, welfare, and

security relied. The resulting Presidential Decision Directive 63 (PDD-63)[3] identified 12 areas critical to the functioning of the country – information and communications; banking and finance; water supply; transportation; emergency law enforcement; emergency fire service; emergency medicine; electric power, oil, and gas supply and distribution; law enforcement and internal security; intelligence; foreign affairs; and national defense – and established structures at the federal level and in the private sector to address vulnerabilities in these critical infrastructures.

PDD-63 raised a number of the key questions surrounding information sharing between the federal government and the private sector that remain today: What is the private sector's willingness and ability to cooperate with the federal government in sharing information? To what extent will the federal government get involved in the monitoring of privately operated infrastructures? What are the legal issues – including privacy and liability – associated with information sharing between the federal government and private sector firms?

PDD-63 established a number of organizations – including the National Infrastructure Protection Center within the Federal Bureau of Investigation (FBI) and the Critical Infrastructure Assurance Office within the U.S. Department of Commerce – to coordinate infrastructure protection efforts nationally. It also assigned a federal lead agency to each of the critical infrastructure sectors. Lead agencies were to collaborate with companies on a sector-by-sector basis to facilitate information sharing on threats, vulnerabilities, incidents, protective measures, and best practices. PDD-63 also called for the private sector to set up Information Sharing and Analysis Centers (ISACs) to "provide an information sharing and analysis capability to support [company] efforts to mitigate risk and effectively respond to adverse events, including cyber, physical, and natural events."[4]

Only a handful of ISACs were created prior to the terrorist attacks of 9/11. Those included ISACs for financial services, information technology, telecommunications, and electricity. After 9/11, the imperative for improved information sharing and greater private sector involvement to address terrorism spurred the creation of new ISACs. By March 2005, there were 15 ISACs, including for chemicals, food, energy, public transit, surface transport, water, and real estate.[5]

While ISACs were established as a result of PDD-63, neither PDD-63 nor the policy changes after 9/11 clearly delineate how the ISACs should operate or how the relationship between the ISACs and the federal government should work. With each industry group free to set up their ISAC as they wished, the ISACs differ widely in quality and structure and in how they are funded, managed, and operated. Some operate as private entities, while others are part of industry associations. Some rely on member fees for funding, while others are sponsored by associations, contracts, or grants.[6]

After 9/11, a number of federal lead-agency designations changed as a result of the government reorganization that created the Department of Homeland Security (DHS).[7] Notably, DHS became the lead agency for information technology and telecommunications, transportation, chemicals and hazardous materials, postal and shipping, and commercial nuclear facilities. Water remained with the Environmental Protection Agency, energy with the Department of Energy, banking and finance with the Department of Treasury, and food and agriculture with the Department of Agriculture.

Since 9/11, sector-specific agencies have provided funding to ISACs to improve their capabilities, expand membership, and support exercises. Sector-specific agencies have hosted outreach events, assisted sectors to organize sector-wide efforts, recommended best practices, and issued information and threat bulletins.[8]

POLICY AND INITIATIVES AFTER 9/11

THE DEPARTMENT OF HOMELAND SECURITY

The Homeland Security Act of 2002, which established DHS, recognized the increased importance of information sharing with the private sector and created new mechanisms and organizations within DHS with that goal in mind. Increased information sharing with the private sector was also highlighted in the National Homeland Security Strategy,[9] the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,[10] Homeland Security Presidential Directive 7 (HSPD-7) regarding critical infrastructure identification, prioritization, and protection,[11] Executive Order 13356 "Strengthening the Sharing of Terrorism Information to Protect Americans," and Executive Order 13388 "Further Strengthening the Sharing of Terrorism Information to Protect Americans."[12]

INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION DIRECTORATE

The Homeland Security Act created an Information Analysis and Infrastructure Protection (IAIP) Directorate as one of the five directorates within DHS. IAIP's mission is to protect critical infrastructure and to serve as a focal point for synthesizing terrorism-related information. IAIP then disseminates information to state and local government and private sector entities. In 2005, Homeland Security Secretary Chertoff announced that he would seek to rearrange IAIP, splitting infrastructure protection into a preparedness directorate

and an Intelligence and Analysis division that would report through a new Chief Intelligence Officer directly to the Secretary.[13]

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

The Critical Infrastructure Information Act of 2002[14] allowed DHS to issue regulations regarding the transmission and protection of critical infrastructure information from the private sector to the federal government. The regulations created the Protected Critical Infrastructure Information (PCII) Program and established uniform procedures for the receipt, care, and storage of private-sector information submitted under the program. In particular, qualifying information is exempt from public disclosure. The goal of the program is to encourage private entities to voluntarily submit to DHS confidential, proprietary, and business-sensitive critical infrastructure information. DHS plans to use the information to assess vulnerabilities, secure critical infrastructure, issue warnings and advisories, and assist in recovery. With non-disclosure protections, the program is meant to allow the private sector to better assist in homeland security without publicly exposing potentially sensitive and proprietary information.

DHS OPERATIONS CENTERS

In addition to the PCII office, DHS also has been seeking to improve information sharing with the private sector by selectively including private sector representation within DHS' round-the-clock operations centers.

The Homeland Security Operations Center (HSOC) serves as DHS' nerve center to (1) collect and fuse information from law enforcement and intelligence sources to help deter, detect, and prevent terrorist attacks; (2) maintain and share daily domestic situational awareness and homeland security monitoring; (3) act as a single point of integration – federal, state, local, and private – for homeland security operational communications and information sharing pertaining to domestic incident management and response; and (4) issue advisories and bulletins concerning threats to homeland security, as well as specific protective measures.

The HSOC disseminates two types of domestic terrorism-related products: threat advisories and information bulletins. Threat advisories contain information about incidents or threats involving critical infrastructure and may indicate changes in readiness, protective measures, or response. Information bulletins communicate more general information relevant to critical infrastructures and are less time-sensitive and specific.

The HSOC comprises more than 35 agencies ranging from state and local law enforcement to federal intelligence agencies.[15] On an ad-hoc basis, it includes

on-site representatives from selected private-sector critical infrastructure sectors, including trucking, rail, chemicals and petrochemicals, telecommunications, and nuclear. For example, the HSOC includes relevant private-sector representatives on site during periods of elevated alert or specific crisis-related or national-security special events, such as the Super Bowl or the presidential inauguration.

In addition to the HSOC, DHS' Transportation Security Operations Center (TSOC) serves as a round-the-clock operations center for transportation security-related operations, incidents, or crises. The TSOC communicates directly with the HSOC and also houses private-sector representatives as needed. The TSOC notifies ISAC leadership and sector coordinators of critical infrastructure events, including notification of imminent threats, dissemination of sector-specific warning products, and changes in national threat level.

HOMELAND SECURITY INFORMATION NETWORK

DHS has launched the Homeland Security Information Network, an Internet-based communications tool that includes directories, email, instant messaging, and geospatial mapping capabilities. The network provides connectivity to all 50 states, Washington, D.C., and more than 50 major urban areas. In June 2004, DHS in cooperation with the FBI launched pilot programs in Dallas, Seattle, Indianapolis, and Atlanta to provide unclassified information to private sector owners of critical infrastructure assets.

DHS PRIVATE SECTOR OFFICE

The DHS Private Sector Office seeks to provide "the U.S. business community with a direct line of communication to the Department of Homeland Security." But the Private Sector Office is not intended nor does it act as a conduit for national security sensitive information, either from industry to government or vice versa. It serves primarily as a liaison office that facilitates interaction between DHS and the private sector and as an outreach office that provides information and education to the private sector regarding the activities of DHS. The DHS Private Sector Office works directly with individual businesses, trade associations, and other professional and non-governmental organizations to share information about department programs and opportunities.

FBI JOINT TERRORISM TASK FORCES

Since 9/11, the FBI has increased the presence of its counterterrorism field offices and operations though Joint Terrorism Task Forces (JTTFs). The JTTFs

are jointly staffed by FBI agents and local law enforcement officials who are assigned to work full time with the FBI. The FBI has increased the number of JTTFs from 35 before 9/11 to 100 in 2005. In addition, as of mid-2005, 56 FBI field offices maintain field intelligence groups to analyze and disseminate information. While none of these efforts explicitly incorporates private sector involvement, the field offices serve as a federal resource to private sector entities on a regional and local basis as needed.

INFORMATION SHARING CHALLENGES

Given the policy changes following 9/11, the creation of the Department of Homeland Security, and the proliferation of information-sharing mechanisms that began in 1998 and accelerated after 9/11, what is the state of public–private information sharing today?

Certainly improvements have been made to information sharing between the government and the private sector since 9/11. DHS has created a number of new offices and programs focused on information sharing with the private sector. At the same time, significant challenges remain. These challenges fall into three broad categories.

First, an unsettled organizational landscape at the federal level and in the private sector sharing mechanisms has left roles and responsibilities for increased and improved sharing unclear at multiple levels of government and, certainly, in the minds of members of the private sector.

Second, issues of trust and risk act as a serious impediment to holders of information for fear that information misuse by other parties might expose them to liability, punishment, or other negative consequences.

Third, the value of improved sharing is often not immediately apparent, leaving private-sector owners of information often seeking a quid pro quo: why should a company give up sensitive information on its facilities if it is not receiving relevant and actionable intelligence information from the government in return?

UNSETTLED ORGANIZATIONAL LANDSCAPE

Far-reaching and rapid organizational change in the federal bureaucracy has posed one of the greatest challenges to improving information sharing with the private sector since 9/11. DHS was designated by the Homeland Security Act to play a lead role in facilitating information sharing with the private sector. While DHS inherited significant assets, including the National Infrastructure Protection Center and the Critical Infrastructure Assurance Office, personnel turnover and disruptions during the transition significantly limited DHS'

effectiveness. According to a report by DHS' Inspector General, to the extent that the certain preexisting federal efforts had achieved "one stop shopping" from the government for critical infrastructure information sharing after 1998, the difficult transition into DHS and associated personnel shortages have hindered information sharing efforts.[16]

The creation of DHS also unsettled the federal landscape by splitting duties for information sharing between industry sectors' traditional regulatory agencies and DHS. This split happened most notably in chemicals and hazardous materials, commercial nuclear plants, and transportation. The fragmentation has contributed to a lack of clarity regarding divisions of responsibility.[17] For example, the Department of Transportation is responsible for regulating transport, but DHS is responsible for transportation security; the Environmental Protection Agency is responsible for regulating chemicals, but DHS is responsible for chemical security.

As a result, private sector officials have complained about confusion, contradictory direction, and duplicative information requests and poor coordination between DHS and other federal agencies. Making matters worse, while DHS has lead responsibility for some sectors, it frequently lacks sufficient or comparable technical expertise in those areas traditionally regulated by other federal agencies, most notably, the Department of Energy, the Department of Transportation, and the Environmental Protection Agency. Near-term staffing shortages have made matters worse, but even when addressed, DHS may never match the sector-specific technical capabilities of counterpart agencies. Lack of deep industry-specific expertise on DHS' part will likely impede robust information sharing between DHS and the private sector.

Paul Kurtz, the former senior director for critical infrastructure protection on the White House Homeland Security Council, said in mid-2004 that "the state of relations between the private sector and DHS when it comes to critical infrastructure is strained, clearly strained, and it's sad."[18] According to other experts interviewed by *Congressional Quarterly*, the causes of the problems include a lack of "a core strategy or a list of priorities. And the near-constant staff changes . . . have led to communication problems."[19]

ISACs were envisioned as the primary node for information sharing with federal authorities, but they have struggled to fill that role. ISACs have suffered from the fact that many have been fee-based membership organizations. Information sent to the ISACs by the HSOC too often has been distributed only to ISAC member companies and has failed to reach non-member companies. As a result, DHS has declined to endorse the ISACs as the primary interface with the private sector. In fact, DHS conspicuously distanced itself from the ISAC model when it promoted the creation of Sector Coordinating Councils. As mandated by executive order (HSPD-7),[20] the councils were set up to be

more inclusive than ISACs and to allow any company or association operating within a sector to become a member for free.

Information Sharing and Analysis Centers and Sector Coordinating Councils remain works in progress. DHS continues to suffer growing pains and must continue to improve its coordination with other federal agencies that have technical expertise and regulatory oversight for particular infrastructure sectors. The landscape for sector-based efforts to share information within industries and between industry and government remains unsettled. A clear model for the organizations, mechanisms, processes, and rules that will best serve information sharing with the private sector is still lacking.

TRUST AND RISK

Even if organizational structures at both the federal level and within industry were more mature, it is not clear that information sharing between the federal and private sectors would be dramatically improved. Much of the reason for this stems from a lack of history and familiarity in exchanging information between the public and private sectors. Corporations have legitimate competitive and liability concerns over the potential disclosure of business-sensitive information, while federal authorities have legitimate concerns over the disclosure of sensitive national security information. According to the Government Accountability Office (GAO), "the benefits [to a company] of sharing information are often difficult to discern, while the risks and costs of sharing are direct and foreseeable."[21]

The primary risks that the private sector perceives around information sharing include the sensitivity of information (for example, information that companies would not want competitors to discover or information related to a break-in that is relevant to ongoing or future law enforcement activities), legal limits on disclosure (such as Privacy Act restrictions on the disclosure of personally identifiable information of companies' customers), and contractual or business limits on disclosure (including non-disclosure agreements with business partners, clients, and customers).[22]

The depth of private sector concerns is reflected in the limited effectiveness of DHS' Protected Critical Infrastructure Information initiative. While the program is one of the federal government's flagship initiatives, it has yet to serve as an effective catalyst for significantly improving information flows. By March 2005, after nearly a year in operation, the PCII office had received only 30 submissions.[23]

For the federal government, an overarching challenge to sharing with the private sector is the security of classified information and a lack of security clearances among private sector officials. To the extent that most sharing with

the private sector takes place, the information shared is unclassified/for official use only, and typically provides only general homeland security information that is not specific enough to be actionable by companies. Providing more sensitive threat information would require appropriate security clearances for private sector recipients of the information. While no specific data are available on security clearances for the private sector, the problem of providing security clearances for first responders and state and local officials provides some insight to the hurdles that would confront comparable efforts to provide clearances for the private sector.

To improve information sharing with state and local officials, Washington has sought to provide expedited clearances to first responders who are members of the FBI's JTTFs. According to the GAO, the FBI has done a good job of processing "top secret" clearances for state and local law enforcement officials who are part of the JTTFs within their target timeframe of six to nine months.[24] It has done a much poorer job of completing lower-level "secret clearances" for first responders who are not part of the JTTFs within their target of fewer than 60 days. According to *Congressional Quarterly*, by early 2005, only two dozen fire chiefs nationwide had security clearances, and critics voiced concerns that the FBI was not moving swiftly enough to expedite applications for fire chiefs.[25] Notwithstanding clearances, a 2003 executive order allows the FBI and other federal agencies to share classified information with first responders who lack security clearances in the cases of emergency.

Part of the difficulty in providing clearances for state and local officials comes from the sheer number required. There are more law enforcement *agencies* in the United States than there are FBI *agents*.[26] The volume problem is similarly evident in completing security clearances for civilian contractors to the Department of Defense, the one area where private sector employees routinely receive clearances.[27] As of 2004, the backlog of clearances was about 180,000, and the average time for completion of a clearance increased by nearly 20 percent to 375 days from 2001 to 2004.[28]

Another challenge posed by security clearances is oversight. In April 2005, Portland, Oregon pulled its police officers out of the Portland JTTF, making it the first city in the country to pull out of the FBI's expanded network of JTTF offices. The decision came, in part, as a result of the FBI's refusal to grant Portland's mayor a top secret clearance. The mayor argued that, unable to see what the Portland policemen on the JTTF saw, he would be unable to exercise full oversight of the police to ensure that officers did not "overstep their authority under state law while acting as federal agents."[29]

The volume and oversight problems would need to be addressed if Washington were to pursue a program of clearances to private sector officials on a meaningful scale. There are hundreds of thousands of critical infrastructure

sites across the United States, a large multiple of the number of state and local law enforcement agencies. The backlog faced by civilian contractors to the Department of Defense would be small compared with the number of critical infrastructure employees who might seek clearances. Furthermore, companies could face oversight problems, similar to those in Portland, unless senior executives and board members also were to obtain clearances that would allow them to exercise oversight over other employees in their organizations who have clearances.

Finally, even if clearances were granted to industry officials on a sufficient scale, information sharing might still be slow to improve. Even within the federal government, where officials have requisite security clearances, information sharing improvements are occurring only slowly. Again, the benefits of sharing are often difficult to discern, while the risks and costs of sharing are direct and foreseeable. For the intelligence community, wider sharing increases the risk of compromising valuable sources and methods.[30] For the FBI, greater sharing increases the risk of compromising a law enforcement investigation. Furthermore, the government culture, developed over decades during the Cold War, has prized secrecy, information control, and data ownership, and it has lived in fear of leaks of classified information.

The obstacles to sharing within the federal government are also relevant when it comes to sharing information externally with state, local, and private sector entities. Even if the problem of clearances could be overcome, it is likely that challenges to information sharing beyond the federal government would remain.

VALUE PROPOSITION: THE QUID PRO QUO PROBLEM

Even if the organizational landscape could become more certain, mutual trust could be strengthened, and sufficient classification and non-disclosure regimes could be established, the information sharing paradigm presumes that the private and public sectors have useful information to share.

A common presumption in the private sector is that the federal government possesses a significant amount of classified information that is specific and actionable. According to the GAO, "most ISACs reported that they believed that they were providing appropriate information to the government but, while noting improvements, they still had concerns with the information being provided to them by DHS and/or their sector-specific agencies. These concerns included the limited quantity of information and the need for more specific, timely, and actionable information."[31] In short, many in the private sector believe that the federal government is withholding valuable information from them.

In truth, this may not be the case. While post-9/11 information-sharing efforts stress the critical need to "connect the dots," the federal government may

not be in a position to provide the dots. U.S. intelligence capabilities declined significantly after the end of the Cold War due to budget and personnel cuts.[32] Even though intelligence budgets have grown since 9/11, it may take at least a decade to rebuild U.S. intelligence capabilities to a sufficient level to, for example, penetrate Islamist terrorist groups and provide adequate intelligence on terrorist threats.[33] As former Central Intelligence Agency (CIA) Director James Woolsey explained, "In intelligence, not only are not all of the dots there, but there are no numbers on them."[34]

The perception that the federal government is withholding information only heightens the reluctance by the private sector to share information with the federal government: why should the private sector give up sensitive information when it is not getting valuable federal information in return?

INFORMATION SHARING BY SELECTED SECTORS

Many of the federal efforts to broadly catalyze information sharing from the top down have had limited success. At the same time, greater sharing of private-sector information with the federal government is occurring on a case-by-case basis, and outside of the PCII program, in certain industry sectors. This is particularly true in aviation, telecommunications, and cyber security, where models of information sharing that existed prior to 9/11 have provided the foundation for current efforts. In air freight and cargo shipping, companies are using the rich availability of supply-chain data to provide federal authorities greater access to information about the shippers that use and packages that travel within their systems.

AVIATION SECURITY[35]

Private airlines began using passenger data – last minute reservations, payment by cash, short or one-way trips – starting in 1996 to assess the risks posed by passengers and checked baggage. In addition, federal authorities have routinely augmented the screening efforts of private air carriers by providing them with government watch list information on persons considered to be threats to aviation security.

Between 1999 and 2001, public criticism and civil liberties concerns led to restrictions on the Computer Assisted Passenger Profiling System (CAPPS I) so that it could only be used to target baggage and not travelers for screening. After 9/11, the restrictions on CAPPS I were lifted to allow it to again be used for targeting both passengers and baggage. In addition, federal authorities have sought to expand passenger screening with additional intelligence and law enforcement information, and to use passenger record data (including name, address, date

of birth, and telephone number) augmented with commercially available consumer data. CAPPS II, as this initiative was known, was scrapped in 2004 under public pressure and privacy concerns after it became known that several airlines had turned over traveler records to federal agencies and defense contractors.[36]

DHS's Transportation Security Administration (TSA) modified the prescreening initiative and renamed it Secure Flight.[37] Under Secure Flight, the federal government would take over from air carriers the responsibility for pre-screening airline passengers. TSA would receive passenger data from the airlines, and compare passenger information against data from a new consolidated watch list database created after 9/11. Additionally, TSA announced that it would test the use of commercially available consumer data (i.e., information that either identifies an individual or is directly attributed to an individual, such as name, address, and phone number) to enhance the efficacy and security benefits of the system.

In spring 2005, a TSA contractor tested the use of personally identifiable commercial data to see if such data could better enable Secure Flight to identify false or stolen identities. The manner in which the contractor collected, used, and stored the commercial data, however, was inconsistent with how TSA had previously publicly described how the program would use commercial data.[38] As a result, "individuals were not fully informed that their personal information was being collected and used, nor did they have the opportunity to comment on this or become informed on how they might exercise their right of access to information."[39] DHS' own privacy office investigated whether the tests violated DHS' own privacy rules.[40] In summer 2005, TSA issued revised privacy notices to more fully disclose the nature of its use of commercial data.

DHS' Data Privacy and Integrity Advisory Committee determined that TSA's commercial data test did not provide a reasonable case for using commercial data as part of Secure Flight. Going further, Congress restricted TSA from using commercial data or databases "obtained from or that remain under the control of a non-federal entity,"[41] which effectively ended the use of commercial data in Secure Flight during, at least, fiscal year 2006.

Secure Flight is a work in progress, and, like its predecessors, it remains controversial.[42] Shifting screening responsibility from the private sector to the federal government and expanding the program to include more personal data has raised criticism from privacy groups and heightened scrutiny on Capitol Hill.[43]

TELECOMMUNICATIONS

Historically, telecommunications companies have cooperated with federal authorities, providing information and access to systems that allow federal

authorities to conduct surveillance. In the 1970s, for example, the National Security Agency (NSA) relied on major telegraph companies to provide copies of messages into and out of the United States.[44] Under the 1994 Communications Assistance for Law Enforcement, U.S. telecommunications carriers are required to make their networks available for wiretaps for domestic law enforcement. While such a requirement does not exist regarding intelligence agencies, the NSA maintains very close relationships with telecommunications and computer industries, even though only a very small group of senior company executives might be aware of such relationships.[45]

In domestic investigations, communication companies typically require court orders before cooperating.[46] But in December 2005, the *New York Times* first reported on a program authorized by President Bush soon after 9/11 allowing wiretaps without warrants on U.S. persons or people geographically located in the United States who might have links to Al Qaeda or Al Qaeda affiliates.[47] News reports indicate that large telecommunications companies, including AT&T, MCI, and Sprint, without warrants, granted access to their systems and provided call-routing information to help physically locate callers.[48] The existence of the program touched off a national furor over the legality of domestic eavesdropping without court approvals as well as a debate over the relative constitutional powers of Congress and the executive branch to authorize intelligence collection in the United States.

In February 2006, the Electronic Frontier Foundation, a privacy-rights advocacy group, sued AT&T, calling the company's participation in the NSA program an unconstitutional invasion of privacy.[49] For companies, the incident raised the potential risk of liability and brand damage due to providing commercial data for intelligence purposes to federal authorities, when a company's customers have certain expectations or even legal claims to privacy protections.

CYBERSECURITY

DHS' National Cybersecurity Division in September 2003 created a U.S. Computer Emergency Readiness Team (U.S. CERT) to provide a national focal point for analyzing computer-based vulnerabilities, disseminating cyber warnings, and coordinating incident and response activities. U.S. CERT links public and private response capabilities to facilitate communication about cybersecurity.[50] It works with the private sector and academia to coordinate responses to major cyber events and to provide information on vulnerabilities, prevention, and remediation to private-sector companies, small businesses, and home users.

DHS created U.S. CERT by integrating several preexisting federal cyber centers and drawing on the capabilities of Carnegie Mellon's CERT Coordination

Center, the country's leading university cybersecurity center.[51] The U.S. CERT is largely modeled after Carnegie Mellon's center but seeks to provide a greater national effort in education and warning for smaller businesses and home users.

The U.S. CERT encourages private-sector companies to report cyber attacks or discovered vulnerabilities. Information specific to the facility and company making the report remains confidential unless explicit permission is granted to release that information. Composite sanitized information is provided publicly so that other companies and individuals can avoid similar attacks and fix similar vulnerabilities.

In January 2004, U.S. CERT started a National Cyber Alerts System to provide cyber security information to the public. The alert system is managed in partnership between the DHS and the private sector. By June 2004, more than 250,000 subscribers were receiving cyber alerts.

SEA FREIGHT: CARGO SHIPPING[52]

Starting in 2003, DHS' U.S. Customs and Border Protection implemented a "24-hour rule" requiring private ocean carriers to provide the U.S. government with extensive data about all containerized cargo shipments – manifests, bills-of-lading, and entry and exit data – at least 24 hours before those containers are loaded onto a U.S.-bound vessel in a foreign port. Data are provided electronically via the Automated Manifest System and are evaluated by DHS' Automated Targeting System (ATS).[53] Each shipment is analyzed and scored according to more than 300 weighted rules derived from targeting methods developed by experienced customs personnel.

The higher the risk score of a shipment, the more the shipment warrants specific attention. The ATS analysis and score is used to decide which containers should not be loaded aboard the vessel at the foreign port, which containers should be inspected at either the foreign port or the U.S. discharge port, and which containers are considered low risk and can be transported without further review. All shipping containers that ATS identifies as posing a potential terrorist threat are inspected, usually with large-scale imaging and radiation detection equipment prior to or upon on arrival at U.S. seaports.

Currently, U.S. importers and foreign exporters are not required to file data that could be used in the security screening process, notwithstanding the fact that the law requires the cargo security screening and evaluation system to be conducted prior to loading in a foreign port. Such data would be valuable as they would provide information beyond what is in carriers' manifest filings. While importers are required to file merchandise entry data with the government, they do not have to do so until after the cargo shipment has already entered

the United States or until it reaches its inland destination, which is too late for security screening purposes.

Customs may eventually require importers to file relevant entry data into U.S. Customs' targeting system 24 hours before vessel loading. Importer data could provide a more detailed and complete picture of cargo shipments and could augment the risk screening currently conducted by ATS.[54] Other information that could improve the quality of cargo risk screening includes more specific and precise cargo description, selling party, purchasing party, point of origin, country of export, ultimate consignee (final recipient), exporter representative, name of broker, and origin of container shipment (name and address of business where container was loaded).

AIR FREIGHT: FEDEX

International freight shipper FedEx provides homeland security officials access to the international portion of its databases.[55] Information provided includes credit card details, shipper name and address, and the package's origin and final destination. Agents cross reference information provided by FedEx with information in government databases. The relationship is mutually beneficial to both parties. With federal assistance and checks against government data, FedEx is better able to flag suspicious packages. Working closely with the government also helps FedEx prevent disruptions to operations and damaging publicity that might ensue if terrorists successfully exploited its systems. For federal officials, cooperation with FedEx provides the ability to see if credit cards have been used in other suspicious transactions and map the activities of and links between persons or organizations of interest.

In addition to providing access to portions of its consumer information database, FedEx encourages its work force to be on the lookout for suspicious activity. It is also building a special computer system to report on suspicious behavior directly to DHS.

FEDERAL INNOVATION

To overcome the problem of few security clearances in the private sector, federal authorities such as DHS and the FBI have sought greater use of "tear line" information. Federal authorities make information shareable by creating "tear line" reports, which contain classified and non-shareable information above the tear line, and then, below the tear line, the unclassified information that can be shared. The problem with this solution to date is that the process of redacting and summarizing classified information to create a shareable unclassified

version of it frequently ends up making the shared information so general as to be not meaningful or actionable to non-federal entities.

Two potential solutions exist to improve the quality of information shared by the federal government with non-government entities. The first solution would be to "write to share" information, which would reverse the typical tear line concept by having government analysts write reports that are shareable in their original form. The information below the tear line would provide additional details that are classified and only accessible with permissions or authentication. While this seems like a minor change, a "write to share" philosophy would require a significant cultural change.[56] Federal officials normally write reports in classified form, and then subsequently extract the information they are willing to share with others. "Writing to share" would force officials from the very start to define what can be shared. This approach can help increase the amount and quality of shareable information and help prevent important information and context from becoming lost in subsequent rounds of redaction and summarization.[57]

Another potential solution that the federal government has begun to implement is for the government to increase its supply of valuable, but non-classified, information. The presidential commission investigating the failure of U.S. intelligence on Iraq's weapons of mass destruction recommended in March 2005 that the CIA establish an office to gather intelligence from "open" or non-classified sources, including newspapers and periodicals.[58] In congressional testimony, witnesses argued that mining unclassified sources could respond to the unique needs of first responders and other non-federal entities, who often lack access to classified information.[59]

DHS is increasingly recognizing the value of open-source information and is now publishing daily open-source infrastructure reports.[60] Open-source intelligence, combined with tear sheet information, has the potential to both increase the quality as well as the volume of information shared by the federal government with the private sector. Success on this front can help mitigate the need for security clearances and may also help address the quid pro quo problem that has contributed to a reluctance by private sector entities to provide information to Washington.

REGIONAL INNOVATION

Recognizing the difficulty of information sharing between the federal and private sectors, efforts are underway to increase regional information sharing between state and local authorities and the private sector. Portland, Oregon, for example, has launched the Connect & Protect^{TM} program to provide

automated, real-time emergency alert notifications from Portland's emergency 9-1-1 system to more than 100 schools and more than 50 homeland security, public safety, and private sector organizations on a secure Internet-based information network.[61] Incident alerts are automatically filtered and targeted to relevant organizations. Users receive alerts of 9-1-1 events and are able to receive additional descriptive detail on incidents, including photographs and maps. The system also provides valuable content to help organizations decide how to respond to the incidents, including materials on precautionary procedures, hazardous materials, evacuation planning, loss prevention, workplace safety, and guidance on training and preparedness.

In the system's first six months of operation between August 2003 and March 2004, it processed 87,000 and delivered 3,500 targeted alerts to network subscribers. The core technology – RAINS-Net – was developed in partnership between the state of Oregon, six research universities, more than 60 technology companies, and a variety of local first responder organizations.[62]

Regional innovation like Connect & Protect is essential to the future of successfully building better information sharing with the private sector. Building systems regionally leverages local geographic relationships to build trusted relationships between the private sector and state and local governments. Over time, as organic regional networks grow, they may be leveraged by federal authorities to build a national "network of networks" for information sharing relationships.

CROSS-SECTOR INNOVATION IN THE PRIVATE SECTOR

Innovative information-sharing projects are also taking place between consortia of companies from multiple industries and the federal government. In one example, technology consulting company C-bridge Corporation is developing a project to improve security at a number of private energy and manufacturing facilities in a concentrated geographic region. The project is aimed at reducing the risk of "insider threats," where current employees or other personnel within a facility might provide aid to terrorists or saboteurs. National labor union and trade groups representing the personnel being screened are also participating in the project.

C-Bridge is using technology from defense contractor Lockheed Martin, personal data from large commercial data aggregators, and watch list data from the federal government to run background checks and perform risk assessments on staff and contract personnel who have access to sensitive manufacturing and energy facilities. C-Bridge's personnel risk assessment pilot is modeled after risk assessment programs the company has built for DHS. The project

utilizes software jointly developed with Lockheed Martin for the Department of Defense to protect classified data and ensure privacy protection for personnel subject to risk screening and background checks.

C-Bridge's approach to data theft seeks to ensure privacy protection by predefining data sharing rules and policies, protecting classified information, and providing continuous auditing and monitoring to ensure compliance with the sharing policies agreed upon by the participants. Continually monitoring how data is being shared allows for constant assessment and mitigation of risk by assuring the companies, personnel, and labor unions that their data are being used only for the purposes for which they are aware and have agreed upon beforehand. If successful, the C-Bridge project can provide lessons for future cross-sector information-sharing initiatives between the private sector and the government.

CONCLUSIONS AND RECOMMENDATIONS

Four years after 9/11, information sharing between the federal government and the private sector remains a significant challenge. While some progress has been made, federal efforts to share homeland security intelligence information with the private sector remain limited and ad hoc. According to the GAO, "DHS has not yet developed a plan for how it will carry out its information-sharing responsibilities. . . . In addition, DHS has not developed internal policies and procedures to help ensure effective information sharing by the many entities within the department that collect and analyze information that may impact the security of our nation's critical infrastructure."[63] According to Zoe Baird, president of the Markle Foundation, there is still no systematic and comprehensive way to integrate the private sector into information sharing.[64]

Private-sector officials have an expectation that that the federal role in protecting their facilities should include as a top priority the transmittal of threat intelligence information. Information provided by the federal government should be consistent, accurate, clear, timely, and as specific about the potential threat as possible.[65] Sharing would be aided by the greater presence of private-sector representatives at DHS operations centers and at regional and field DHS and FBI offices. Sharing would also be aided by a greater use of tear line and open source information, and the growth in distribution networks like the Homeland Security Information Network and Portland's Connect & Protect. Sharing is made more difficult by the problem of getting large numbers of security clearances for private sector personnel, by fear of improper disclosure of classified information, and by the fact that federal authorities may not possess actionable or specific intelligence. Finally, it is imperative that

the federal government be better coordinated and, to the greatest extent possible, speak with one voice. In several instances since 9/11, that has not been the case, with the FBI and DHS releasing uncoordinated and conflicting messages regarding threats to the financial sector, oil refineries, and mass transit.[66]

The sharing of sensitive corporate information in the other direction – from companies to the federal government – also suffers from growing pains. The primary broad mechanism established to catalyze private-sector submissions of information to the federal government (the PCII Program) has gained little traction due to risk aversion by the private sector. Companies fear improper or inadvertent disclosure by the government of information sensitive to individual companies. When private industry and government both have a sense that the other side is holding information back, it perpetuates a lack of trust and creates an unproductive quid pro quo mentality in which each side waits for the other to be more forthcoming as a condition for sharing more themselves.

An unsettled organizational landscape at the federal level and within the private sector has not helped matters. DHS remains understaffed, suffers high personnel turnover, often lacks sufficient technical expertise, and is frequently poorly coordinated with counterpart agencies that possess greater industry expertise. Within the private sector, the primary information sharing nodes – ISACs and Sector Coordinating Councils – vary widely in quality and operations, are not yet mature, and lack clearly defined roles, responsibilities, and sharing protocols.

Given continuing challenges in broad-based sharing efforts, the sharing and innovation that does take place will likely continue to develop independently on a sector-by-sector or regional basis. Furthermore, sharing programs are more likely to occur in sectors where several conditions are met: First, programs for providing corporate information to federal authorities are more likely when there exists an established history of information exchange, often via a regulatory relationship. Preexisting relationships have provided the framework for experimentation in the passenger aviation sector, telecommunications, and cybersecurity.

Second, companies will be more likely to share corporate information when doing so can help them better protect their own assets, prevent misuse of their systems, and detect and reduce costs associated with crime or fraud. With cybersecurity, making up-to-date vulnerability information available to other companies and the federal government provides awareness of common vulnerabilities, a public good that benefits all community members. In aviation, screening passengers prevents airplanes from being hijacked or destroyed. With sea and air freight carriers, sharing shipper and supply chain data with federal authorities improves companies' ability to detect and prevent crime and fraud as well as potential terrorist attacks.

Third, companies are more likely to share information with federal authorities where existing geographic and regional relationships between firms can be leveraged, as in the case of Portland's Connect & Protect and C-Bridge's pilot program with a consortium of manufacturing and energy firms. Over time, pilots and regional programs have the potential to provide a model for or contribute to the creation of national programs. Just as importantly, innovative pilots help to build and strengthen trust relationships across the public–private divide.

At the same time, information sharing from the private sector to the federal government has the potential to become problematic where a company's sharing is not required by regulation or where it does not meet a company's direct self-interest in protecting its own assets against criminal or terrorist attacks. Information sharing where the primary goal is to provide intelligence information to the government – as in the case of cooperation by telecommunications companies on eavesdropping without warrants – has exposed AT&T to legal liability and brand reputation issues relating to the privacy rights of its customers. Similarly, the use of commercial consumer data to augment the screening of airline passengers has led to censure and protests of the program over privacy rights. FedEx's information sharing with federal authorities also raises privacy and legal issues. According to a former CIA official, "the new cooperation between business and the government takes place in a legal 'gray zone' that has never been tested in court. [These] relationships could undermine existing privacy laws."[67]

Faced with legal risk and ambiguity, many companies – including FedEx rival United Parcel Service, General Motor's OnStar in-vehicle emergency communications system, Internet service provider Earthlink, and cable service provider Cox Communications – say that, as a matter of policy, they do not disclose customer information to federal authorities without a subpoena, warrant, or court order.[68]

Improving information sharing with the private sector is a work in progress. The challenges to information sharing between government and the private sector are widely recognized. The federal government and the private sector must make better progress on a number of recommendations that have been made by both government and private-sector groups over the past several years.[69] The government needs to develop a comprehensive and coordinated national plan to facilitate information sharing regarding critical infrastructure protection. That plan needs to clearly delineate roles and responsibilities, craft data exchange and handling mechanisms and processes, define interim objectives and milestones, set timeframes for achieving objectives, and establish means to measure progress. Industry should become better integrated into the full government intelligence cycle (requirements, tasking, analysis, reporting, and

dissemination). At the same time, the government must aggressively increase its analysis, use, and dissemination of open-source information both within and outside of government. Federal authorities should increase their industry expertise and better harness private-sector analytical capabilities to better develop sector-specific information and intelligence requirements.

While policy and institutional reforms since 9/11 have placed top priority on improving sharing between the government and the private sector, policy reforms must translate into meaningful and durable changes in behavior. It is critical to identify the mechanisms, rules, procedures, and incentives/disincentives that will promote information sharing and foster the creation of organizations, programs, and systems that will support it. Sharing information must become part of the DNA of the national security, intelligence, and homeland security communities, federal state and local officials, and the private sector. Viewing the private sector as an equal partner in detecting, preventing, and responding to terrorist attacks must become second nature to intelligence, law enforcement, and other government agencies. Dramatically improving information sharing between the government and the private sector will take creativity and persistence from the executive branch, Congress, state and local officials, and business leaders.

NOTES

1. Bergen 2002.
2. The 9/11 Public Discourse Project, which comprises the continued efforts of the National Commission on Terrorist Attacks Upon the United States (known as the 9/11 Commission), issued a report card in December 2005, in which it gave the federal government a grade of "D" for its information sharing efforts (see 9/11 Public Discourse Project 2005). Similar concern over progress in information sharing with the private sector was expressed in congressional testimony by Zoe Baird, President of the Markle Foundation, before the House Permanent Select Committee on Intelligence (Baird 2005).
3. U.S. Department of Justice 1998.
4. Government Accountability Office (GAO) 2004b.
5. GAO 2004b, Table 2.
6. GAO 2004b, Table 2.
7. These changes were reinforced by the National Strategy for Homeland Security in July 2002 and Homeland Security Presidential Directive 7 in December 2003.
8. GAO 2004b.
9. Office of Homeland Security 2002, p. xi: The National Strategy for Homeland Security identifies five major initiatives in this area: integrate information sharing across the federal government; integrate information sharing across state and local governments, private industry, and citizens; adopt common "meta-data" standards for electronic information relevant to homeland security; improve public safety emergency communications; and ensure reliable public health information.

10. Office of the President 2003, p. xi: Information Sharing and Indications and Warnings. This strategy identifies six major initiatives in this area: (1) define protection-related information sharing requirements and establish effective, efficient information sharing processes; (2) implement the statutory authorities and powers of the Homeland Security Act of 2002 to protect security and proprietary information regarded as sensitive by the private sector; (3) promote the development and operation of critical sector Information Sharing Analysis Centers; (4) improve processes for domestic threat data collection, analysis, and dissemination to state and local government and private industry; (5) support the development of interoperable secure communications systems for state and local governments and designated private sector entities; and (6) complete implementation of the Homeland Security Advisory System.
11. White House 2003a. "Coordination with the Private Sector: (25) In accordance with applicable laws or regulations, the Department and the Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the Department and Sector-Specific Agencies shall collaborate with the private sector and continue to support sector-coordinating mechanisms: (a) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and (b) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices."
12. White House 2005.
13. Chertoff 2005.
14. See sections 211–214 of the Homeland Security Act.
15. A full list of HSOC participants includes the Federal Bureau of Investigation, U.S. Coast Guard; U.S. Postal Inspection Service; Central Intelligence Agency; U.S. Secret Service; Washington, D.C., Metropolitan Police Department; Defense Intelligence Agency; Federal Protective Service; New York Police Department; National Security Agency; U.S. Customs and Border Protection; Los Angeles Police Department; U.S. Immigration Customs Enforcement (including Federal Air Marshal Service); U.S. Department of Energy; U.S. Environmental Protection Agency, Drug Enforcement Administration; U.S. Department of the Interior (U.S. Park Police); Bureau of Alcohol, Tobacco, Firearms, and Explosives; U.S. Department of Defense; U.S. Department of State; U.S. Department of Transportation; U.S. Department of Veterans Affairs, National Capitol Region; Transportation Security Administration; National Geospatial-Intelligence Agency; U.S. Department of Health and Human Services; Federal Emergency Management Agency; National Oceanic Atmospheric Administration; and the Department of Homeland Security's Public Affairs, Office of State and Local Coordination, Science and Technology Directorate, Geo-spatial Mapping Office, Information Analysis Office, and Infrastructure Protection Office.
16. According to the DHS Inspector General, significant personnel shortages inhibited the integration process of DHS' Information Analysis and Infrastructure Protection directorate in its first years of operation. See Department of Homeland Security 2004.
17. For example, GAO noted a lack of clear roles for DHS and Department of Transportation when it came to transportation security (see Government Accountability Office 2003c). To clarify roles, GAO recommended that the Department of Transportation and DHS enter a memorandum of understanding, a recommendation with which DOT and DHS disagreed.
18. Starks and Andersen 2004.

19. Starks and Andersen 2004.
20. See White House 2003.
21. GAO 2004b, p. 10.
22. ISAC Council 2004b. See also Government Accountability Office 2004b. For text of the Privacy Act of 1974, see http://www.cftc.gov/foia/foiprivacyact.htm, accessed November 2005.
23. From Knake 2005.
24. GAO 2004d. The FBI's goal is to complete the processing for secret security clearances within 45 to 60 days and top secret security clearances within 6 to 9 months, beginning with the FBI headquarters' receipt of the application from the FBI field office. Since September 11, about 92 percent of applications for top secret security clearances were processed within the FBI's timeframe goals. During this same period, about 26 percent of secret security clearance applications were processed within the FBI's timeframe goals. The FBI was more successful with processing top secret security clearances within its stated timeframe goals than secret security clearances, in part because the FBI often assigns greater priority to processing applications for state and local Joint Terrorism Task Force (JTTF) members.
25. Madigan 2005.
26. Hamilton 2005.
27. Government Accountability Office 2004c.
28. Government Accountability Office 2004c and Harris 2004.
29. McCall 2005.
30. Hoekstra 2005.
31. GAO 2004b, p. 9.
32. Commission on the Roles and Capabilities of the U.S. Intelligence Community 1996. See also Federation of American Scientists 2004.
33. See, for example, Flynn 2005b.
34. Marks 2004.
35. For a thorough history and overview, see Elias et al. 2005.
36. See, for example, Goo 2004.
37. GAO 2005a.
38. GAO 2005b.
39. Berrick 2006.
40. Singel 2005b.
41. The Department of Homeland Security Appropriations Act, as cited in Berrick 2006.
42. CBS News 2005. See also Singel 2005a.
43. GAO 2005a.
44. McCullagh and Broache 2006.
45. McCullagh and Broache 2006.
46. Cauley and Diamond 2006.
47. Risen and Lichtblau 2005.
48. Cauley and Diamond 2006.
49. Associated Press 2006.
50. Yoran 2004a. See also Yoran 2004b.
51. The Carnegie Mellon CERT Coordination Center serves as a major reporting center for Internet security problems, provides technical advice and coordinates responses to security compromises, identifies trends, works with other security experts to identify solutions to security problems, and disseminates information to the broad community.

The coordination center also analyzes product vulnerabilities, publishes technical documents, and presents training courses.

52. Ortolani and Block 2005.
53. Although ATS inputs go well beyond advance manifest information, the scope and reliability of the cargo information currently received under the "24-hour rule" is reinforced by the Trade Act Final Rule published on December 5, 2003. This rule mandates advance electronic cargo information inbound and outbound for all modes of transportation.
54. See Coalition for Secure Ports (undated).
55. Block 2005.
56. Sarkar 2004.
57. Dempsey 2004.
58. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction 2005.
59. Harrington 2005.
60. See, for example, http://www.globalsecurity.org/security/library/news/2005/02/dhs_iaip_daily_2005-02-28.pdf, accessed November 2005.
61. See http://www.rainsnet.org/files/PDF/RAINS_Connect_and_Protect_Fact_Sheet.pdf, accessed November 2005.
62. See http://www.rainsnet.org/downloads/RAINS_Fact_Sheet.pdf, accessed November 2005.
63. Government Accountability Office 2004b, pp. 9–10.
64. See, for example, Baird 2005.
65. Government Accountability Office 2005d.
66. Frank 2004; Strohm 2005; Mintz and Schmidt 2004; Sherman 2005; and Leavitt 2005.
67. Block 2005.
68. Block 2005; McCullagh and Broache 2006.
69. Ralyea and Seifert 2004. Also see GAO 2004a,b; and ISAC Council 2004a,b.