6-1-2009

Information Sharing for Infrastructure Risk Management: Barriers and Solutions

Henry H. Willis
hwillis@rand.org

Genevieve Lester
Georgetown University

Gregory F. Treverton

Follow this and additional works at: http://research.create.usc.edu/published_papers

Recommended Citation
Willis, Henry H.; Lester, Genevieve; and Treverton, Gregory F., "Information Sharing for Infrastructure Risk Management: Barriers and Solutions" (2009). Published Articles & Papers. Paper 27.
http://research.create.usc.edu/published_papers/27

This Article is brought to you for free and open access by CREATE Research Archive. It has been accepted for inclusion in Published Articles & Papers by an authorized administrator of CREATE Research Archive. For more information, please contact gribben@usc.edu.
Information Sharing for Infrastructure Risk Management: Barriers and Solutions

Henry H. Willis; Genevieve Lester; Gregory F. Treverton

To cite this Article Willis, Henry H., Lester, Genevieve and Treverton, Gregory F.(2009) 'Information Sharing for Infrastructure Risk Management: Barriers and Solutions', Intelligence and National Security, 24: 3, 339 — 365

To link to this Article: DOI: 10.1080/02684520903036925
URL: http://dx.doi.org/10.1080/02684520903036925
Information Sharing for Infrastructure Risk Management: Barriers and Solutions

HENRY H. WILLIS, GENEVIEVE LESTER AND GREGORY F. TREVERTON

ABSTRACT There is a public interest in ensuring that infrastructure systems are appropriately protected and prepared for disruptions. While infrastructure protection is usually viewed as a public responsibility, infrastructure risk management actually requires a high degree of cooperation between the public and private sectors, particularly in the sharing of information about risks to infrastructure. Discussions with Chief Security Officers across sectors of the US economy reveal the complexity of the task, as they describe at length the private sector’s requirements of multiples types of information about a range of potential threats. While the US government has established many mechanisms for sharing information, barriers remain that inhibit both the private and public partners from obtaining the information needed to protect infrastructure. Overcoming these barriers requires new thinking about the intelligence generation process, the mechanisms and practices upon which the process relies, and the responsibilities of those in the private sector who participate in it.

Introduction

On 13 September 2001, Commandant Thad Allen (then Vice-Admiral) was confronted with a complex decision. Days earlier, the most tragic terrorist attacks on the US had brought New York City to its knees. Unseen to many, the 11 September attacks invoked a full-scale maritime response to secure infrastructure and transport residents of New York off of Manhattan. The US Coast Guard (USCG) closed New York Harbor to all vessels except those involved in the response to the terrorist attacks. Amid efforts to resume normalcy in New York, it quickly became incumbent upon the Coast Guard to decide when to open the harbor to commercial vessels. This required balancing ensuring that the harbor was safe and secure and allowing it to serve the purpose for which it exists, that is, facilitating the efficient movement of goods, commodities, and people. In the end, the decision to open the harbor was not made because security concerns subsided but because of the linkages between the harbor and the energy sector. The harbor was opened because heating oil reserves in Albany, which are
supplied through New York harbor and serve large portions of the Northeast, were reaching dangerously low levels.¹

Commandant Allen’s decision to reopen New York Harbor emphasizes the typically unseen, seamless integration of infrastructure systems upon which we depend daily. By one count, infrastructure constitutes 18 separate but overlapping physical and virtual systems that produce services that are needed for the operation of society.² The energy and water that we use relies on electricity generation, transmission and distribution; nuclear reactors; dams and waterways; and public and private water treatment and distribution systems. We have food and household goods because transportation systems bring them to grocery stores and other commercial facilities from farms, our banking and finance systems manage transactions that we use to pay for them, and waste management systems to take away what we don’t use. In turn, these systems do business by relying on the products of chemical manufacturing and refineries, communications and information technology, critical manufacturing, and postal and shipping companies. Finally, through facilities and services (some of which are national icons) the government ensures that we have an environment that includes safe secure communities, good public health, and strong legal and financial institutions.

This infrastructure faces threats and disruptions daily. The technology that constitutes it can fail. Hurricanes, earthquakes and other natural disasters can cause physical damage. Intentional attacks from explosives, weapons of mass effects, or malicious cyber-activity can bring these systems to a halt.

When the infrastructure fails it can affect individuals and the economy as a whole, presenting risks that must be assessed and prudently managed. Thus, there is a public interest in ensuring that these infrastructure systems are appropriately protected and prepared for disruptions. This is a daunting task because taken together infrastructure systems constitute thousands of facilities across the United States. While there is a public interest in managing infrastructure risk, doing so is not purely a public responsibility. The vast majority of infrastructure facilities are owned and operated by private interests. As a result, infrastructure risk management requires cooperation between the public and private sector. One area in which this is particularly true is in the sharing of information about risks to infrastructure, especially intentional man-made risks such as terrorism.

Infrastructure owners and operators are usually all too well aware of the consequences to their business when events and accidents cause damage or disruption to their facilities. By the same token, they typically understand

where vulnerabilities exist within facilities and how threats to infrastructure can impact these vulnerabilities. What they often don’t know, however, is what the threat of some disruptions are – especially those related to intentional attacks by domestic or international terrorist groups. Government intelligence analysis could be a critical source of information about these threats in cases where it is able to provide warning about imminent attacks or changes in the general nature of threats that infrastructure faces.

Like the private sector, the government also does not have all the information it needs. As part of missions to protect and prepare communities, federal, state and local agencies allocate resources to identify threats, protect communities from them, and develop capabilities to effectively respond and recover when a disaster or attack occurs. Local, state and federal intelligence provides information to identify threats but does not provide sufficient information to guide decisions of how best to protect against, respond to or recover from these threats. The heart of the terrorist threat to infrastructure is that terrorists are the ultimate of what the Pentagon calls ‘asymmetric threats’. They do not attack the United States where it is strong but rather where it is weak. They are looking for vulnerabilities and weaknesses. The 11 September hijackers, for instance, didn’t come to their plan because they were airplane buffs. Rather they had done enough tactical reconnaissance to know their plan could succeed. They had found seams in America’s defense.

In making decisions about how resources should be allocated, the Department of Homeland Security (DHS) has adopted the use of risk analysis as the guiding framework. This creates the natural requirement for information from the private sector. Assessing risk requires combining judgments about the threat with those about vulnerability and consequences of an attack. In some cases, with shoes on the ground, the managers of infrastructures may have better information about the local threat than do government authorities. In any case, though, those managers will surely know much more about vulnerabilities and consequences than the government can.

Commandant Allen’s decision to open New York harbor provides an example of how information flows between the public and private sector can work. Following the attacks, the government provided instructions to private companies about how the flow of goods would be impacted. Based on this information, infrastructure owners and operators were able to anticipate the consequences of the disruptions to their ability to provide essential services. As it became clear that the disruptions were threatening to limit the supply of heating oil, information-sharing mechanisms allowed the

\]

private sector to alert the USCG of the issue and the government could respond to balance security with effective operation of infrastructure services.

It is widely recognized that effective two-way information-sharing is required to protect US infrastructure. However, it is equally widely recognized that current efforts to share information are not uniformly as effective as the example of information sharing at the Port of New York and New Jersey following 11 September. To develop solutions for fixing the problems of information-sharing for infrastructure risk management, we need to first understand the problem.

To that end, we reached out to Chief Security Officers (CSOs) representing a variety of critical infrastructure sectors. These professionals discussed with us the reasons they look for information about terrorism threats, what sources they find most useful, and challenges they confront when sharing information with the government. To put these views in perspective, we also reviewed documentation about current information-sharing activities and processes sponsored by federal, state, and local authorities.

These discussions revealed many dimensions to problems of information-sharing. Collecting information from the private sector requires coordinating, organizing, and analyzing thousands of disparate information feeds. Local, state, and federal law enforcement face challenges when sharing classified intelligence from the top down and incident reports from the field up. Finally, the public sector faces another set of challenges when considering how to share insight from classified and unclassified intelligence with the private sector. The goal of this article is to describe the nature of the challenges of this third type of information sharing (i.e., between the government and the private sector) and as a result the characteristics of effective solutions for improving it.

We begin by discussing why the private sector wants information from the government and what types of information is desired. Next, we describe several barriers to effective communications. Then, we outline what efforts are underway to facilitate information-sharing between the public and private sector. We conclude with recommendations for doing better by working around some of the existing barriers to sharing information and analysis.

---


6Interactions with Chief Security Officers were not through a formal survey. Rather we reached out to Chief Security Officers through personal contacts, especially RAND advisory boards, for largely unstructured interviews by phone and in person. During the interviews we discussed topics such as the importance of information sources for their responsibilities, what information sources they found useful, whether information from federal agencies was useful, what contacts they had with those agencies, and whether they found classified information useful.
What Information Does The Private Sector Want?

Jennifer E. Sims describes intelligence as an interaction between two parties engaged in a competitive process. Using this broad definition, one can envision many reasons why intelligence is important to the private sector. Companies compete with each other for profit and revenues. The firm that is able to produce goods more cheaply, of higher quality, and with greater consistency has an advantage in capturing a larger share of the market.

In the competition for business, firms face many threats. Theft of goods from warehouses and shipping facilities accounts for billions of dollars of losses annually before products reach stores. Natural disasters and terrorist attacks can damage property and physical systems. The resulting disruptions from these events can result in delayed and canceled shipments. Executives from multinational firms travel the globe securing and strengthening business relationships and expanding the firms’ markets. Intelligence analysis can help the private sector understand the nature and magnitude of threats like these. However, firms are not interested in studying threats as an academic pursuit. They do so because they must make strategic, operational, and tactical decisions, the success of which depends on a sound awareness of the threat environment.

Firms Make Strategic, Operational, and Tactical Choices

Strategic decisions are those that define why a firm operates in the manner that it does. They are characterized by decisions directing operations towards corporate goals and mission. They are made relatively infrequently but are reviewed and updated on a regular basis. For example, manufacturing companies must decide from which companies to source supplies, in which companies to establish manufacturing, and in which companies to establish retail or wholesale operations.

Firms then make operational decisions to establish procedures and deploy resources to accomplish progress towards goals and objectives. For example, ports, chemical facilities, and airports must decide how many people and which types of technology are required to conduct broad-area surveillance to protect facilities. As another example, shipping firms must establish procedures for screening shipments and ensure adequate staff to complete the procedures effectively.

Finally, when adverse events occur, firms must make tactical decisions on how and when to respond. For example, after a bombing at an overseas facility, firms may decide to evacuate or relocate employees. Increasingly, firms think of their businesses as processes, ones that can be reconstituted if need be, rather than as facilities that necessarily must be rebuilt. Firms may choose to increase security at similar facilities or other facilities that face similar threats to those involved in an event. If given specific warning about

---

imminent threats, firms may also decide to increase security, evacuate employees, or move operations elsewhere.

Information Needs and Sources Depend on Decisions Being Made

Security professionals require different types of knowledge to make each of these decisions (see Table 1). At the tactical level, security officers require specific information about threats to the people and facilities they are responsible for protecting. This can be in the form of information about events that have recently occurred or knowledge of imminent danger to an area, firm, or facility that is similar to those they are responsible for. Generally, the security professionals we spoke with indicated that they obtain this information from local and federal law enforcement agencies. To the extent this occurs, it is facilitated by existing relationships that were developed through past employment or participation in regional preparedness planning groups. In that sense, it is very much akin to the tactical information that US military units transfer to coalition partners in ongoing operations. Private sector security officers will rely on the history of the relationship; they don’t need to know exactly where the information came from. In the case of knowledge of events that have occurred, more often than not, the news is available over national media by the time they are contacted by law enforcement authorities.

Operational decisions are often related to advising corporate officers of whether, how, and how much to invest in security. For example, the recent chemical facility securities regulations require plants to review, document, and, if deemed necessary, increase the level of security at facilities. At facilities that represent hundreds of millions to billions of dollars in capital investments, security improvements can easily cost tens of millions of dollars. For corporate leaders to assess the return on these security investments they must have a sense of how likely attacks will be. This type of decision problem exists across many industry sectors, and among the security professionals we met there was a general consensus that credible information did not exist to guide this decision-making. Indeed, from a risk management perspective, companies would like just what traditional intelligence services are most loathe to provide (even if the barriers to sharing could be overcome) – numerical estimates of threat likelihoods. Even the best models in the insurance industry – like that used by Risk Management Solutions – rely on expert elicitations to frame front-end probabilities of a terror attack. As a result, several of the companies we talked to said that while they value back-end damage estimates of those models, they pay less attention to the front-end threat probabilities.

Finally, corporate leaders also look to security professionals to guide them on how security impacts enterprise risk management. This is specifically relevant when companies consider expanding operations into new countries. In such cases, it is important for firms to understand the stability of security

---

<table>
<thead>
<tr>
<th>Type of decision</th>
<th>Examples of decisions being made</th>
<th>Examples of types of information needed</th>
<th>Examples of how information is obtained</th>
<th>Perceived adequacy of information available</th>
</tr>
</thead>
</table>
| Tactical         | Whether to stop production at a chemical plant  
                        Whether to evacuate executives from a country  
                        Whether to increase the presence of security guards at facility gates  | Has a similar type facility been attacked?  
                        Is there knowledge of an imminent threat in the area of the facility?  
                        Is there knowledge of an imminent threat to facilities like this one?  | Local law enforcement  
                        FBI  
                        National news | Good |
| Operational      | Whether to install additional cameras for perimeter surveillance  
                        Whether to raise or secure a building’s ventilation inlets  
                        Whether to relocate chemical storage to a less accessible location within a facility | What is the likelihood of attacks using [mortars, anthrax, radiation dispersal devices, etc.] in the next five years?  
                        What is the likelihood of attacks on facilities like those we own/operate in the next five years? | Generally not available from commonly used sources | Poor |
| Strategic        | Whether to build a manufacturing plant in a new country  
                        Whether to acquire equity in a foreign company  
                        Whether to revise business continuity plans to consider additional scenarios | What types of weapons are terrorists groups attempting to obtain?  
                        Is organized crime or terrorism widespread or rising in the country?  
                        Are there indications that the stability of a country’s government is changing? | Subscription intel. services  
                        Government and think tank analysis  
                        Overseas Security Advisory Council | Good |
and political institutions in countries, the level of terrorism, and the nature and extent of organized crime. It seemed that this type of information was generally available from several sources. Those most frequently mentioned in our discussions with security professionals included subscription intelligence services, unclassified reports by government agencies and think tanks, and participation in information sharing activities like the State Department-organized Overseas Advisory Council (described further in the next section).

**Classified Information Is Rarely Needed or Desired**

In discussions about what information the private sector needs, we did not hear a strong desire to have more access to classified information sources. This is worth noting because senior security professionals at private firms often have experience with how the intelligence community works and what type of information is available. They often obtained this experience through careers at the FBI, CIA or other intelligence organizations. Thus, the lack of desire to have greater access to classified intelligence is not a result of lack of knowledge of what exists. It has more to do with lack of utility of the knowledge to their responsibilities. There are two primary reasons for this.

First, the information needs described above and presented in Table 1 do not in principle require passing knowledge of information that tends to cause intelligence to become classified. Specifically, the private sector is not interested in how or from where information is obtained, provided that the intelligence community is able to provide an assessment of the credibility of the information. Examples would include the advisories from the 2005 London bombings and the 2004 threats against US financial institutions. All were unclassified and thus without indications of the sources. The latter were at least specific to sector and location: Washington, New York and New Jersey.

Second, in many organizations, senior executives do not have access to classified information. For example, among the professionals we spoke with, it was rare that their CEO, CRO, CFO, CIO, Board of Directors, or other corporate leadership held security clearances. Thus, if the security professionals did have access to specific classified intelligence, they would not be able to share it within their firm with those responsible to act on their guidance.

**What Are the Private Sector Barriers to Sharing Information?**

The reasons for reticence in sharing information on the part of the private sector only compound the challenges imposed by the government’s preoccupation with protecting secret information. On the private sector side, there are four principal concerns – over leaks of proprietary information to competitors, over losing customers or investors if company vulnerabilities become public, over the liability they might incur in, for instance, reporting suspicious behavior to public authorities, and over the risk that voluntary disclosures will bring to bear regulatory procedures, for instance, over environmental effects.
Notice that all of these concerns have as much or more to do with what happens to information once disclosed to some government body as to the simple fact that the government collected it. It is not as important that the government knows the information as it is what the government does with the information. That is, in all cases the concern is that information will be passed, or leak, from its original recipient and purpose to others, perhaps unpredictably. (If the same recipient has two missions – for instance, both information gathering and enforcement – the concern is built in from the beginning.) As a result, all the information-sharing mechanisms discussed in the next section, and especially those intended to reach out to the private sector, grapple with the balance between using information and protecting it.

Concern about leaks of proprietary information to competitors is straightforward but perhaps muted somewhat in the homeland security realm because the information in question will concern vulnerabilities, not competitive advantages. Yet it is imaginable that disclosing information about vulnerabilities in processes, for instance, might inadvertently disclose something of competitive value to competitors. In the case of chemical processes, for instance, knowledge of how much chemicals and of what type could provide information to competitors regarding what processes are being used and how inventories are managed.

The second concern is closely related. If disclosures don’t provide advantage to competitors, they could affect markets or frighten off customers or investors. In one case in Southeast Asia, the UK-based Aegis Defence Services reported on anticipated future links between Islamic terrorists and maritime criminals in a maritime threat-vulnerability study. Despite dismissals of the validity of this report by Singaporean and Western officials, the Lloyds Joint War Council designated the Straits of Malacca as an area of Enhanced [Terrorism] Risk. This designation created the opportunity for insurance companies to levy a war surcharge on ships transiting the waterway.9

Liability is a third concern. Companies could incur liability in several ways. If they reported a vulnerability that terrorists (or Mother Nature) later exploited, they could be liable for resulting damages. In one case in our interviews, a major package delivery company was approached about asking its drivers to be on the lookout for suspicious activity. The company was inclined to agree but sought protection from the government against any liability incurred. When that could not be provided, the initiative died. In that case, the liability presumably might have arisen if the reported suspicious activity led to police activity or other negative consequences for what turned out to be innocent behavior.

Finally, there is the concern that information will be passed not to competitors or customers but to other government agencies. Our interviews, for instance, surfaced the concern that for private companies to disclose risk information would be seen as admitting a liability. If this disclosure triggered a reporting requirement under Securities and Exchange Commission’s

---

disclosure regulations, the result could ultimately lead to public disclosure of information that the security community (both public and private sectors) would prefer not occur. This might create an incentive not to share information. In another instance, our interviews with shippers revealed concern about sharing manifests with US Customs and Border Protection lest disputes arise about appropriate tariffs. Perhaps the most likely of these cases would be regulatory agencies responsible for environmental or safety issues. It would be important for decisions driven by the risk management framework to take into account, for instance, any vulnerabilities entailed in the presence of hazardous materials at particular facilities. Yet if that information were passed to the Environmental Protection Agency, regulatory issues might arise.

What Are the Public Sector Barriers to Sharing Information?

On the government side, procedures were developed, especially in intelligence but also in law enforcement, to protect information, not share it. The holy grail of intelligence is protecting ‘sources and methods’. Thus, the balance in all intelligence procedures is tipped toward protecting information, not moving it quickly around. Law enforcement takes more account of the need to move information – and it knows that in the end, to convince a court, it will have to make public some of how it knows what it knows. But along the way there is abiding concern lest inadvertent disclosures of information compromise ongoing cases. Before 11 September, it took a court order to get information from (secret) federal grand juries passed to intelligence analysts.

As a result, while in public presentation the challenge of sharing intelligence with state and local authorities down to the cop on the beat often is portrayed as a problem of technology, it is not. Technology can help. But the challenge is one of policy, not hardware. From the outside, the security issues look daunting, but insiders seldom mention them. They are so used to them that they hardly notice – a possible indicator of how hard change will be. People don’t recognize the extent to which they are constrained by current procedures. The asymmetry is that no one ever has to account for the cost of security procedures in other than money. No one ever has to say ‘I can make this document more secure, but the price will be that three local officials who should see it won’t, or won’t in time’. As a result, the crust of security procedures only deepens, and while the watchword in the government is ‘risk management’, the actual practice is still better characterized as ‘risk avoidance’.

10 These issues are discussed in much more detail in Gregory F. Treverton, *Intelligence for an Age of Terror* (Cambridge: Cambridge University Press 2009), especially chapter three.

11 The FBI was required to provide information to the Director of Central Intelligence (DCI) but only if that information was ‘essential to the national security’, and only ‘upon the written request’ of the DCI. National Security Act of 1947, 50 U.S.C. 403, Sec. 102 (e). The FBI also was responsible for protecting material before federal grand juries, and while sharing was possible, in practice information came to be shared only with a court order.
In one sense, the problem of security is less pressing now, or at least should be in principle. During the Cold War, intelligence was very dependent on a small number of collectors, so any single-point exposure was deeply damaging. Arguably, that is less so now with many, varied targets and much more information.\textsuperscript{12} Even if that is true, however, it still means that intelligence will have to recognize, as Silicon Valley has, that innovations that confer advantage are fleeting. If advantage is to be maintained, it will require a short cycle in producing new innovations.

The 9/11 Commission recognized that the issues are less technical than policy related in nature. It recommended creating a government-wide ‘trusted information network’ to share information horizontally, on the model suggested by a recent task force organized by the Markle Foundation.\textsuperscript{13} For the WMD Commission, the December 2004 bill’s provisions on that score, though, raised as many questions as they answered. The bill created a program manager to build such a network for the war on terrorism. Yet that manager was to sit outside the intelligence community and report to the president – a recognition that the ‘information-sharing’ problem runs well beyond intelligence. In the end, the program manager for what is called the ‘Information Sharing Environment’ (ISE) effectively works for the Director of National Intelligence (DNI), which is more straightforward even if it does limit the manager’s mandate.

ISE’s mission statement is a terse description of the problem:

Today’s ISE consists of multiple sharing environments designed to serve five communities: intelligence, law enforcement, defense, homeland security, and foreign affairs. Historically, each community developed its own policies, rules, standards, architectures, and systems to channel information to meet mission requirements. Prior to 9/11, the need for coordinated and trusted interagency partnerships was not universally recognized and thus gaps and seams existed in the sharing of information across all levels of government . . . We envision a future ISE that represents a trusted partnership among all levels of government in the United States, the private sector, and our foreign partners.\textsuperscript{14}

\textsuperscript{12}One example to the contrary, reported in a book, validated by the 9/11 Commission and cited by President George W. Bush, seems to have been an ‘urban legend’. That was the assertion that Osama bin Laden stopped using his satellite phone to communicate with subordinates immediately after a newspaper article indicated the United States was using it to locate him. See Glenn Kessler, ‘File the Bin Laden Phone Leak Under “Urban Myths”’, \textit{Washington Post}, 22 December 2005, p.A02, available at <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/21/AR2005122101994_pf.html> (accessed 3 April 2009).


Yet the ultimate difficulty is not mandate but policy. Framed as ‘information-sharing’, the solution is one the nation cannot get to from here. Rather the challenge is what might be called ‘coproduction’, jointly producing information across the federal structure.\textsuperscript{15} It requires reshaping security to effectively confront the threats ahead – which requires perhaps the ultimate change in culture. It will have to been done step by step, resting at each step on solid analysis that current procedures, while they may make particular documents safer, make the nation less safe.

A number of smaller proposals can at least make a start. For instance, intelligence analysts, like other professionals, want to play at the top of their games, so their reports inevitably begin with the most classified – and thus least sharable – information. The 9/11 Commission suggested the opposite, starting any report by separating information from sources and writing first at the level that can be most easily shared. (Some agencies, like the National Security Agency, do write different versions but typically start with the most classified, then adjust those ‘downward’ in classification.) If intelligence consumers wanted more, they could query the system under whatever rules were in place, leaving an audit trail of requests. Now many, perhaps most, potential consumers would not even know what to ask for.

Already, many agencies have reached out for translators into pools of people they would not have tapped before, such as immigrants who have spent much of their adult lives abroad. Certainly, it is possible to imagine different kinds of clearances for different kinds of jobs. In 2008, then-DNI, Mike McConnell, talked of getting people, even first- and second-generation Americans, clearances within a month, then following them carefully with what would amount to ‘lifecycle monitoring’ – that is, constant surveillance.\textsuperscript{16} He also set in motion a review of classification policy.\textsuperscript{17}

The military is creative during coalition operations in using ‘tear line’ intelligence, so that information can be separated from indications about the source and transferred to non-American coalition partners. Documents literally are torn in half, with the information passed to partners but not the source information. There is no reason that the FBI and Department of Homeland Security (DHS) cannot be comparably creative in thinking of ways to get information to uncleared partners. Now, the principal means the federal government has for working with state and local authorities are the FBI Joint Terrorism Task Forces. Yet those are built around FBI communications, and so require state and local participants to be cleared at the top secret level.

On the collection side, the terrorist threat to the homeland is impelling agencies, FBI and the DHS in particular, to think of their officers as

\textsuperscript{15}We owe the term ‘coproduction’ to our friend and colleague, Lt. John Sullivan of the Los Angeles County Sheriff’s Department.


‘embedded collectors’. That should open up new thinking about how to move information to and from their own sub-units, ones in which clearance levels vary. Before 11 September, FBI agents collected a lot of information but concentrated on the portion that was immediately relevant to the specific case they were investigating. As embedded collectors, they would recognize that information they collect has value beyond the case, to others if not immediately to them. In addition to the FBI, DHS has 18,000 agents in Customs and Border Protection, 15,000 employees in Citizenship and Immigration Services, and 48,000 screeners in Transportation Security – all potential intelligence collectors – not to mention 600,000 state and local law enforcement officers. The revision of the main executive order governing intelligence, EO 12333, in July 2008, authorized DHS to ‘collect, analyze, produce and disseminate information, intelligence and counterintelligence to support national and departmental missions; and to conduct and participate in analytic or information exchanges with foreign partners and international organizations’.18

How Is Information Shared?

The ISE program manager’s mission statement neatly stated the problem. Yet what seems to have happened is that information-sharing mechanisms have proliferated without much clarity about how effective any of them are or about coordination between them. With increased reliance on information-sharing as the ‘mantra’ of the post-9/11 world, resources have been thrown at already established initiatives while new ones have sprouted up all over the country. The sheer number and variety of these initiatives illustrates the scale and complexity of the problem. Entrenched agencies have been forced to change focus and mission based on wave after wave of reform, while they have also been prevailed upon to integrate new flows of information, new consumers, and new producers of intelligence. Primary information-sharing objectives have focused on integrating the public and private sectors, but also have prioritized integrating information flows vertically, between the federal, regional, and local levels.

Moreover, not only has the intelligence community expanded and adapted to include these new arrivals, but the initiatives themselves have also been forced to adapt to the shifting priorities of decision-makers responsive to competing demands of emerging threat and community requirements. This section illustrates a range of information-sharing initiatives with special relevance to the private sector. The initiatives described are by no means comprehensive of information-sharing mechanisms in place. They instead were selected because they are active, reasonably well described in public sources, and as a set of illustrative examples provide a view of the ways initiatives are organized, the variety of information-sharing relationships

that exist, and the constraints and problems endemic to carrying out their information-sharing missions successfully.

**Joint Terrorism Task Forces (JTTFs)**

These, organized by the FBI, are the most established of information-sharing mechanisms. Described in an important Markle Foundation report as ‘decentralized analytic nodes’, they combine the efforts of federal, state, and local law enforcement officers in order to detect and prevent terrorist attacks through the collection and sharing of intelligence information.\(^{19}\) The FBI is the lead agency in the partnerships and contributes funding and counter-terrorism training to the task force agents.\(^{20}\) The various participants bring their own agency information networks to the JTTF, thus allowing direct and informal sharing of information. The activities of the JTTFs differ from traditional law enforcement investigation to include longer-term intelligence gathering activities such as surveillance, monitoring, and source development.\(^{21}\) One of the key functions of the JTTFs is ‘deconflicting’ investigations – that is, distributing cases to JTTF member agencies for their investigation, and then monitoring progress to ensure that the investigations don’t work at cross purposes to one another.

JTTF responsibilities reflect local and regional security needs and threat environments. Their configurations and memberships also reflect historical local and regional relationships between agencies.\(^{22}\) The nature of the threat also determines which set of agencies will be drawn into a specific investigation. For example, beyond traditional law enforcement agencies, the Secret Service, Immigration and Naturalization Service (INS), Federal Aviation Administration (FAA), or Drug Enforcement Agency (DEA) could participate in an investigation.\(^{23}\) JTTFs have varied responsibilities depending upon the level of the agency partnership. For example, in a RAND survey conducted several years after 9/11, it was reported that most local law enforcement agencies valued the JTTFs for their assistance with information-sharing (and training), while actual joint participation in an investigation was likely to take place at the state agency level.\(^{24}\) In July


\(^{22}\)Ibid.


\(^{24}\)Ibid., pp.36–37.
2002, a National Joint Terrorism Task Force was established to coordinate the work of the JTTFs. Staffed by representatives from 40 agencies, its role is to serve as a ‘point of fusion’ for terrorism information. It also serves to coordinate information-sharing between participating agencies and between headquarters and regional level JTTFs.25

The terrorism task force structure itself is not new – they began in 1980 in New York – but after the attacks on 9/11, FBI leadership began to focus on them as a dynamic and flexible approach to counterterrorism. The number of JTTFs increased from 34 to over 100 between 2001 and 2007. While generally deemed effective in their investigative and coordination role, the JTTFs also face constraints. One is security clearances. Because they work in FBI spaces, if state and local (and private) task force participants are to be full members of the team, they need security clearances at the level of their FBI counterparts. Not only is that process slow, but, understandably, many elected officials and senior local police officers chafe at having to be ‘cleared’ by the FBI.

Fusion Centers

The creation of fusion centers is a newer initiative, promoted by DHS, and built to some degree upon interagency relationships that preceded the post-9/11 focus on counterterrorism. Similar to the JTTFs, fusion centers co-locate analysts from several agencies in order to facilitate the fusion of several streams of intelligence information. The responsibility of the centers is to fuse foreign intelligence with domestic information in order to facilitate improved policy decision-making on issues of counterterrorism, crime, and emergency response.26 The membership of these centers is determined by local and regional need and security priorities. Although they are state-created and state-based law enforcement entities, fusion centers are, in most cases, at least partially funded by a DHS program, the Homeland Security Grants Program. DHS has assisted in the funding of 38 fusion centers where law enforcement and DHS Office of Intelligence and Analysis officers collaborate, gathering and analyzing data in an effort to reduce the threat at a local/regional level.27

Domestic information is drawn from a range of sources, including local law enforcement, public health, and, increasingly, the private sector. The fused information is then used to guide the allocation of security resources as well as to provide a link between federal and state/regional/local authorities.28 The reasoning behind tightening the relationship between the federal and sub-federal authorities is, from the perspective of DHS, to

26This and the next paragraph draw on Todd Masse, Siobhan O’Neil and John Rollins, Fusion Centers: Issues and Options for Congress, CRS Report for Congress (6 July 2007) pp.11, 29–30. The quote is from p.29.
28Masse et al., Fusion Centers, p.5.
improve federal level situational awareness by providing access to non-traditional intelligence information sources. From the perspective of the state and local entities, the relationship – in principle – facilitates greater insight into federal security priorities by improving information flow and intelligence analysis capabilities. In furtherance of this goal of a tighter bond between the federal and local/regional levels, DHS has committed to embedding federal analysts within the fusion centers.

The fusion centers are intended to complement the JTTFs. If JTTFs work on cases once identified, the fusion centers are meant to assemble strategic intelligence at the regional level and pass the appropriate information on to the investigators in the task forces. In practice, the fusion centers are very much a work in progress. Their missions vary based on regional requirements and resources. Organizationally, they differ considerably from one another in terms of organization, management, personnel, and participation. Communications between centers ranges from problematic to non-existent. The centers’ access to technology and intelligence information is uneven. Not all fusion centers even have state-wide intelligence systems. According to the CRS, ‘The flow of information from the private sector to fusion centers is largely sporadic, event driven, and manually facilitated.’ They also do not all have access to law enforcement data. The problem of interoperability of systems that was widely criticized immediately after 9/11 still exists.

Security clearances remain a bar to sharing, though the situation is improving. In that same CRS study, roughly half the staff of the average fusion center (totaling about 27), had Secret clearances, about six had Top Secret and one had Secret Compartmented Information (SCI). Because of the huge number of information systems and the resulting duplication, analysts are inundated with floods of information of variable quality. Reviewing incoming information is thus extremely time-consuming, all the more so because there are few standards or guidelines about which open source information to monitor or how. Further, although there is much rhetoric expended on the importance of a cyclical information flow between the fusion centers and the federal intelligence community, the information cycle tends to rather one directional. From the perspective of the fusion centers themselves, the value of information becomes opaque once sent to the federal intelligence agencies. This lack of a feedback loop creates both resentment and inefficiency in the relationship between federal entities and the fusion centers.

Moreover, as outward signs of the terrorist threat wane, many of these centers are changing their focus from a pure counterterrorism mission to an

---

30 Masse et al., Fusion Centers, p.20.
31 Ibid., p.29.
33 Ibid., p.30.
‘all-hazards’ approach as priorities change at the local and regional level. This change reflects the simple fact that for most localities, terrorism is not the, and perhaps not even a, major problem. And that shift to an ‘all-hazards’ approach may not be a bad thing as the ‘domestication’ of the terrorist threat means that it more and more resembles organized crime.

Finally, there has been lingering concern about issues of civil liberties and fusion centers, mainly because of public perception of lack of transparency in their operations. A range of reports, including one published by the American Civil Liberties Union (ACLU) in December 2007, have brought up concerns that the expansion of intelligence gathering and sharing in these centers threatens the privacy of Americans. Some of the concerns raised by the ACLU stem from the wide range of participants involved in the fusion centers, including the private sector and the military. The report argues that breaking down the many barriers between public and private sector, intelligence and law enforcement, and military and civil institutions could lead to uncontrolled civil liberties abuses; particularly if a strong and clear legal framework isn’t established to guide operations within the centers.

Homeland Infrastructure Threat and Risk Analysis Center

The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), an analytical unit within DHS, merges information about terrorist intentions and capabilities with data about the vulnerabilities of US critical infrastructure, such as transport or telecommunications systems. It coordinates with the nation’s 18 private infrastructure sectors in the interest of transmitting information about the terrorist threat to a range of consumers, including in the private sector. It is the joint program office for assessing risk to critical infrastructures and key resources. HITRAC is a ‘joint infrastructure-intelligence fusion center’, operating between the Office of Infrastructure Protection and the Office of Intelligence and Analysis, which provides threat and risk assessments. Because HITRAC’s consumers include the private sector in addition to a range of recipients on the federal,

---


state, and local levels, issues of classified information arise. Interestingly, HITRAC avoids that problem, one that runs throughout this paper, by special legal authority to distribute assessments at the For Official Use Only (FOUO) level to owners of critical infrastructure. It also has a program through which executives from the private sector may be cleared at least to the Secret level so that they may review threat assessments.

Some of the products include Quarterly and Annual Suspicious Activity Assessments, which provide strategic, national level assessments of suspicious activity that has been reported to DHS. Interestingly, the private sector has engaged with HITRAC in establishing a baseline, or common understanding, of what constitutes ‘suspicious behavior’. This problem of standardization runs throughout most of the information-sharing initiatives. Other products generated by HITRAC include Infrastructure Intelligence Note – warning infrastructure owners/state/local partners about issues pertaining to security – and Joint Homeland Security Assessment, Strategic Sector Assessments, and State and Regional Threat Assessments.

InfraGard

InfraGard is an FBI information-sharing/analytical partnership program, which began in 1996 in the Cleveland FBI field office. Its original goal was to infuse the Bureau’s initiatives in cyber-security with input from academia and private sector information technology firms. The focus broadened after 9/11 to include not only cyber-threats but also physical threats to critical infrastructure. The InfraGard program distinguishes three types of threats: unstructured threats – generally hackers; structured threats – organized crime, terrorism; and national security threats – foreign intelligence agencies, information warriors.

InfraGard chapters, composed of businesses with security clearances, are linked to FBI Field Offices and coordinated through an FBI Special Agent Coordinator. The coordinator in turn works with the Supervisory Special Agent Program Managers in the FBI Headquarters’ Cyber Division. From 1998 InfraGard was managed by the National Infrastructure Protection Center (NIPC); project management moved to the Cyber Division of the FBI in 2003. The program has remained under the auspices of the FBI although NIPC was transferred to the Department of Homeland Security.

A national Board of Directors, composed of seven elected members, represents InfraGard’s membership to the FBI. In addition to the broader chapter interests, more specific threats are addressed in Special Interest Groups, focusing on specific types of infrastructure. Examples include

---

38Statement for the Record of Robert B. Stephan, Assistant Secretary for Infrastructure Protection, DHS, United States House of Representatives Committee on Homeland Security Subcommittee on Transportation Security and Infrastructure Protection, 23 March 2007.


40Smislova statement, p.4.

41<http://www.infragard.net/>.

42<http://www.infragard.net/>.
agriculture, computer security, energy, finance, transportation, and telecommunications. In principle, the chapters facilitate communication with local, state, and federal agencies, and provide training and information regarding the threat of terrorism and cyber crime. Chapters hold meetings to discuss threats and other security-related activities, and some take on education initiatives as well as scenario-planning.

**Information Sharing and Analysis Centers**

In parallel with the endeavors mentioned above, the federal government has encouraged the formation of industry ISACs (Information Sharing and Analysis Centers), which also bridge the gap between government and the private sector. Such groups had long existed in some sectors, like communications and transport, and now, in principle, span 17 critical infrastructure and key resource sectors. The ISACs, along with Sector Coordinating Councils, serve both as central points of information sharing within each of the sectors and also to act as the liaison to the federal government. Their main functions are to funnel threat information to facilities and receive and collect information from facilities. For instance, the Chemical Sector ISAC has supported DHS information-sharing efforts since the Department’s inception and includes over 600 individuals representing more than 430 different chemical companies.43

One interesting model, and part of the inspiration for the ISACs, is the Overseas Security Advisory Council (OSAC), established in 1985 by the US Department of State to foster the exchange of security related information between the US government and the US private sector operating abroad. Administered by the State Department’s Bureau of Diplomatic Security, OSAC has developed into an enormously successful joint venture for effective security cooperation. Through OSAC, the American private sector, including colleges and universities, receives timely information on which to make informed corporate decisions on how best to protect their investments, facilities, personnel and intellectual property abroad.

Professional security officers of the State Department’s Bureau of Diplomatic Security lead the OSAC program overseas. During meetings of overseas OSAC Councils, members share information on local and regional security issues. OSAC currently encompasses the 34-member core Council, an Executive Office, over 100 Country Councils, and more than 3,500 constituent member organizations and 372 associates.

Among the objectives of the Council as outlined in the Charter are to establish a continuing liaison and provide for operational security cooperation between the State Department’s security functions and the private sector; to facilitate information-sharing between the State Department and the private sector regarding developments in the overseas security environment; and to provide materials and training for program implementation.

43For more, see <http://www.dhs.gov/xnews/releases/press_release_0616.shtm>.
Terrorism Early Warning Groups

Beyond the broader reaching mechanisms listed above, there is a range of local and regional counterterrorism initiatives – some of which existed before the surge in emphasis on counterterrorism after the attacks on 9/11. One, the Terrorism Early Warning (TEW) model, designed in Los Angeles under the auspices of the Los Angeles Sheriff’s Department in 1996, has provided a distinctive model of a regional approach to counterterrorism.\(^{44}\) The TEW brings together dozens of public agencies in order to facilitate the sharing of information on the local level.\(^{45}\) The original concept was developed in an attempt to fill in gaps in traditional intelligence structures and developed on the military concept of Intelligence Preparation of the Battlefield to produce a tailored Intelligence Preparation for Operations process.\(^{46}\) As one of the originators of the TEW, Lt. John Sullivan, points out the TEW model was itself a foundation for other post-9/11 counterterrorism fusion efforts mentioned in this paper, such as the fusion centers, including the Joint Regional Intelligence Center in Los Angeles.\(^{47}\)

One of the innovations of the TEW model was its networked approach to the fusion of intelligence, uniting regional law enforcement, fire departments and public health agencies that deal with the threat of terrorism. Another innovation is its approach to intelligence fusion and its development of the Transaction Analysis Cycle that assists in anticipating threats and developing intelligence collection strategies.\(^{48}\) In the Los Angeles TEW, the group is composed of analysts from local, state, and federal agencies who work on the production of intelligence products dealing with all phases of response. As Sullivan notes, the objective of the TEW is to identify emerging threats and provide early warning regarding them by integrating the analytical product of an interagency team.\(^{49}\) This is the concept of intelligence ‘co-production’ mentioned earlier in this piece. The LA TEW is organized into six cells:

- **Officer-in-Charge (OIC):** this cell provides direction and sets intelligence requirements. The OIC also is responsible for interacting with the incident command entities.


\(^{45}\)‘Local Anti-Terrorism Information and Intelligence Sharing: Information Sharing Overview’, <www.llis.gov>.

\(^{46}\)See also John P. Sullivan, Hal Kempf and Jamison Jo Medby, ‘Understanding Consequences in Urban Operations: Intelligence Preparation for Operations’, INTSUM Magazine XV/5 (Summer 2005).


\(^{49}\)Ibid.
- Analysis/Synthesis: this cell coordinates net assessment activities and develops an iterative collection plan. This cell is also responsible for developing the outcomes of the cells’ analysis into actionable intelligence products.
- Consequence Management: this cell assesses the consequences of the threat.
- Investigative Liaison: this cell coordinates with criminal investigative entities in addition to the intelligence community.
- Epidemiological Intelligence (Epi-Intel): this cell is responsible for disease surveillance and further activities that help with the investigation regarding disease outbreak.
- Forensic Intelligence Support: this cell supports the work of the other cells using technological tools such as sensors, detectors, geospatial tools and cyber means.\(^50\)

The TEW has also formed partnerships with private sector organizations responsible for critical infrastructure. Information-sharing and interoperability are the core benefits of this model. Information is derived from a full spectrum of sources – classified, sensitive, and open source.\(^51\) This organization is assisted by a network of Terrorism Liaison Officers from the relevant agencies. The larger view of the TEW model is that each will be one node in a network that will extend across the United States and, ultimately, to other countries. The TEW model has been developed in other regions of California – including Riverside/San Bernardino, Orange County, Sacramento, San Diego, and the East Bay (San Francisco Bay Area). TEW groups have also emerged farther afield in Washington State, Oklahoma, Ohio, and Louisiana.\(^52\)

**Information-Sharing Portals**

There exists a family of DHS portals at different levels of classification. The Homeland Security Information Network (HSIN) is restricted but not classified. According to DHS officials, HSIN-Secret (HSIN-S) is the portal through which the Department provides intelligence products up to the collateral SECRET classification level to State and local partners. HSDN is analogous to the Department of Defense’s Secret Internet Protocol Network (SIPRNET). HSIN-Intel is a portal at the Secret Compartmented Intelligence (SCI) level that DHS uses primarily to disseminate current homeland security intelligence information and integrated intelligence assessments derived from both DHS and intelligence community sources to law enforcement, first responders, and private sector homeland security partners.\(^53\)

---

\(^{50}\)Ibid., p.4.
\(^{51}\)Ibid., p.2.
\(^{52}\)Ibid.

HSIN, launched in 2004 and upgraded in 2008, is a web-based communications network that supports real time computer-based counterterrorism communication linking all 50 states and 50 urban areas. DHS views the HSIN as its primary vehicle for the two-way transmission of sensitive but unclassified information.\(^{54}\) The network provides incident and pre-incident information mapping and imagery tools, situational awareness and terrorism analysis. A document library contains a range of reports from federal, state, and local levels.\(^{55}\) Law enforcement, emergency response and fire departments, homeland security, and counterterrorism communities share information through this network. The network provides analytical capabilities and real-time connection with the DHS Homeland Security Operations Center as well as private and public sector organizations responsible for dealing with security, the terrorist threat, and emergency response.\(^{56}\)

HSIN was to be built on the foundation of the Joint Regional Information Exchange System (JRIES), which had been created by police agencies and the Defense Intelligence Agency (DIA) in 2002. However, in a microcosm of the problems of information-sharing, it broke apart over competing purposes. DHS wanted to focus all information in one location, and so sought to include homeland security and other non-law enforcement officials in the network. Yet there was apparently at least one leak of case-sensitive information from the network, and the police sought to develop a barrier around the law enforcement portions. The focus of the expanded network is to support counterterrorism efforts by engaging information and human resources at the state, local, and federal level in order to facilitate information-sharing and quicker response to threats.\(^{57}\)

HSIN is organized into a grouping of portals that addresses the specific concerns of the individual groups the network serves. Interestingly, users access the HSIN directly through the Internet where each user can access the counterterrorism portal. In order to gain access to the other portals, users must be members of the network.\(^{58}\) Examples of the other portals include: law enforcement analysis; HSIN Law enforcement; HSIN critical sectors; and HSIN Critical Infrastructure Warning Information Network (CWIN), a


\(^{58}\)Ibid.
network that connects entities that are critical to infrastructure needs in case of national emergency.\textsuperscript{59}

HSIN-Intel, at the SCI level, includes a handful of types of intelligence products:

- Assessments and Studies: some of these are DHS, others are not. Most are not highly classified, but the latest National Intelligence Estimates relevant to terrorism and homeland security, for instance, are posted.
- Advisories: these are all Unclassified/For Official Use Only (U/FOUO), as they are intended for the full range of DHS customers, from the intelligence community to the public. The latest posted were from the 2005 London bombings and the 2004 threats against US financial institutions. Most of these advisories are joint FBI-DHS.
- Homeland Security Intelligence Reports (HSIR): these communicate intelligence from DHS components to headquarters.
- Homeland Security Intelligence Articles (HSIA): these are all sources, intended to assess, clarify or consolidate new or previous intelligence.

HSIN has raised concern about potential privacy and civil liberties issues, in part because of the origins in JRIES, which includes DIA. DIA, an organization expressly forbidden from gathering information domestically due to its direct connection to the Department of Defense, remains linked into HSIN.\textsuperscript{60} Broader civil liberties concerns focus on the potential for gathering information on law-abiding and yet controversial political/social organizations.

HSDN allows government agencies to share security information at the Secret level. The purpose is also to share information with private sector partners who also have this level of clearance. The DHS intention was to have HSDN installed in all of the fusion centers where DHS officers were assigned. Interestingly, at the point of installation, only DHS officers would have access to this network.\textsuperscript{61}

How Can Information-Sharing Be Improved?

This listing of sharing mechanisms, which could easily be extended, underscores the problems with information-sharing and the bafflement it causes all around, perhaps especially to the private sector. In this short listing of mechanisms, at least three seem to overlap, if not duplicate, each other in protecting infrastructure – InfraGard, HITRAC, and the ISACs. The most established mechanism, the JTTF, is perhaps the least accessible and least interesting to the private sector, given the requirement of clearances.

\textsuperscript{59}Ibid.
\textsuperscript{60}Ibid.
and the focus on investigations. Including all the virtual portals, there seem to be too many initiatives chasing too little useful information. Put differently, a torrent of information, often redundant and of widely varying usefulness, easily overwhelms the capacity to digest it. As the CRS report put it: ‘fusion center officials remarked that their staff could spend all day, every day reviewing all the information posted on these systems, and still not be confident they had seen all relevant and/or unique data’. In a RAND assessment of domestic intelligence in the United States, the National Counterterrorism Center (NCTC) generally was regarded as doing relatively well at ‘connecting the dots’ of threat information, but it was seen as much better at moving information upward, toward the president, rather than downward toward states and localities, let alone the private sector.

If the first frontier after 9/11 was building better cooperation among federal intelligence agencies, and the second was reaching out to state and local authorities, the third is building cooperation with the private sector, especially managers of ‘public’ infrastructure. Our interviews and the review of existing arrangements suggest a number of recommendations for doing better on this third frontier.

Reconceive Information-Sharing

The first recommendation is conceptual, reconceiving what is called ‘information-sharing’. So long as it is thought of that way, there is little hope of improvement. The conception of ‘information-sharing’ is triply bad. First, the language implies that agencies ‘own’ their information, sharing it only as they see fit; in that sense, the language only reinforces the legacy of the existing stovepipes. Second, that language implies that if only information could move more freely, all would be well. Third, it implies that the challenge of sharing intelligence with state and local authorities, down to the cop on the beat, is technical, ensuring enough information pipes to move information freely. It is not. Technology can help. But the challenge is one of policy, not hardware.

The challenge needs to be thought of as coproduction – that is, jointly producing useful information and analysis across America’s far-flung federal system. What came through loud and clear in our interviews – as it had in earlier ones RAND conducted – is that the flow has to go in both directions. Private sector infrastructure managers, like state and local authorities, will not long participate if they feel that the federal government is only hunting for information. The cycle has to be a cycle, with private managers not only feeling that the federal government is handling any information they provide

63See Gregory F. Treverton, Reorganizing US Domestic Intelligence: Assessing the Options (Santa Monica, CA: RAND Corporation 2008).
carefully but also that they know what happens to any information they provide and are getting useful information and analysis in return.

Comparative advantage should be the guiding principle: what private managers have are shoes on the ground – that is, deep knowledge of their operations and vulnerabilities. What they don’t have is either classified information or an easy ability to notice developments elsewhere that might be suggestive of threats to them. Most, save the largest companies, don’t have much ability to assemble and analyze information. On those scores, the federal agencies have an advantage. The system for jointly producing information and analysis should build on the relative advantages. It is imperative that private companies both have a clear sense for what happens to information they provide and feel they receive valuable information in return.

Consolidate Mechanisms

Even a partial listing of existing mechanisms demonstrates too many INs – information networks – chasing too little information. To some extent, letting a thousand flowers bloom made sense, especially in the early years after 9/11, when it wasn’t clear what was possible and what would be useful. The plethora of initiatives, some top down and some bottom up, provided a kind of natural experiment. Now, however, both state and local authorities, and private sector managers, feel, in turn, neglected and overwhelmed. Some consolidation seems in order, and this could be a role for the Director of National Intelligence, in cooperation with DHS and FBI. A starting point would be to begin where this paper leaves off, and do a careful survey of state authorities, local authorities, and private infrastructure managers to determine which existing information-sharing mechanisms they found useful and which not.

Be Creative in Business Practices

If existing business practices, especially in the federal intelligence agencies, are a critical obstacle, those practices will not be changed wholesale overnight. The accumulated crust of security procedures is too deep. But they can change. Creativity is possible. Homeland security officials clearly can be as creative as the US military in designing the functional equivalents of ‘tear sheets’, so that classified information can be separated from its source. A number of possible innovations have already been mentioned. HITRAC, for instance, manages to turn all its warnings into the FOUO level, which is a form of the larger task of getting intelligence agencies to work, first, at the lowest – and thus most shareable – level of classification.

So far, in visiting the DHS-sponsors fusion centers, there seems to be remarkably little evidence of shared best practice either in exploiting open source information or in fusing information from various sources. The same seems true of the private sector, again with the exception of the largest firms. The Los Angeles county Joint Regional Intelligence Center, for instance, is an impressive facility, with TV screens all around; yet the screens, ranging from CNN to Al Jazeera, seem to reflect more the interests and tastes of individual analysts than any sense of best practices in exploiting open sources. There would seem an important role for DHS
in reaching out to the fusion centers, and beyond them to the private sector, in recommending both sources and techniques for exploiting and fusing information from them.

**Consider Firewalls and Indemnification**

Because liability concerns loom so large in the concerns of the private sector, the federal agencies should consider both firewalls and limited forms of indemnification. In thinking of the former, the Centers for Disease Control and Prevention is an interesting possible model. It has built a reputation for receiving information from the private health sector and dealing carefully with it. At the most ‘public’ level, it faces a trade-off akin to that in the homeland security realm – receiving and providing information to those who need it without causing undue panic. Its challenge may be somewhat easier than that faced in homeland security to the extent that the public level is most important, as it seeks to understand the threat posed by particular diseases without having unprocessed bits of data cause public panic. Yet it also is in the position of seeking data from health care providers that might put them at a competitive disadvantage or even invoke liability. In the homeland security realm, some firewalls might reassure companies that data they provided would be used for the purpose intended, and only transferred to other agencies or other purposes on conditions the companies understood in advance.65

By the same token, blanket indemnification is not in the cards, nor desirable if it were. But it is worth considering indemnification in some circumstances. The package delivery service mentioned earlier is a case in point, for the local delivery driver no doubt has ‘domain awareness’ of his locality that could complement that of local law enforcement in the same area. It surely is worth looking for ways, including indemnification, to add that driver to the local eyes and ears in the fight against terrorism.

**Empower CSOs**

As hinted earlier, chief security officers are a critical link in the process of jointly producing information and assessment. As both corporate operations and security threats have globalized, their role has evolved from securing sites (and protecting against insider theft), to preparing travelers for foreign travel, to, now, participating in corporate decisions about how to protect and hedge against a range of threats from Mother Nature to terrorism. Again, the CSOs at the largest companies run very sophisticated operations. One we interviewed, from a very large company, had come to his position from a federal intelligence agency. He said he had expected his work in the

---

65For an example of a careful agreement about sharing information at the federal level, see Memorandum of Agreement between the Attorney General and the Director of National Intelligence on Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center of Terrorism Information Contained within Datasets Identified as Including Non-Terrorism Information and Information Pertaining Exclusively to Domestic Terrorism, 2008 (unclassified).
private sector to be very different from the government but was surprised to
find it less different than he imagined. What he meant was that his company
was big and extended enough to be government-like in its opportunity not
just to respond to but to shape its operating environment.

CSOs need to be thought of as full partners in the process of risk
management. Sometimes, to be sure, CEOs treat them almost as cut-outs,
letting the CEO disclaim knowledge of particular issues or threats. At others,
CSOs still are relegated to narrow responsibilities. But making them full
partners means, first, carefully surveying what it is they need, then, second,
trying to find ways to work with them to provide the information and
assessment that will make the central participants in corporate decisions not
just about short-terms alert statuses and precautions but also longer-term
investment and business process decisions. They are central to crossing the
third frontier in securing the homeland.

Acknowledgements
This research was supported by the RAND Center for Terrorism Risk
Management Policy and the United States Department of Homeland Security
through the National Center for Risk and Economic Analysis of Terrorism
Events (CREATE) under grant number 2007-ST-061-000001. However, any
opinions, findings, and conclusions or recommendations in this document
are those of the authors and do not necessarily reflect views of the United