National Infrastructure Advisory Council

Intelligence Information Sharing

Final Report and Recommendations*

January 10, 2012

Alfred R. Berkeley, III
Chairman
Pipeline Trading Systems, LLC

Wesley Bush
Chairman, President and
Chief Executive Officer
Northrop Grumman

Philip G. Heasley
President and Chief
Executive Officer
ACI Worldwide

James B. Nicholson
President and Chief
Executive Officer
PVS Chemicals, Inc.

James A. Reid
President
CBRE Group, LLC
Eastern Division

Michael J. Wallace
Former Vice-Chairman and
Chief Operating Officer
Constellation Energy

*The Final Report and Recommendations are subject to deliberations by the National Infrastructure Advisory Council

Table of Contents

About the NIAC

The National Infrastructure Advisory Council (NIAC) provides the President of the United States with advice on the security of the 18 Critical Infrastructure and Key Resources (CIKR) sectors and their information systems. These critical infrastructure sectors span the U.S. economy and include the Banking and Finance, Transportation, Water, Energy, and Emergency Services Sectors, among others. The NIAC also advises the lead Federal agencies that have critical infrastructure responsibilities and industry sector coordinating mechanisms. Specifically, the Council has been charged with:

- Enhancing cooperation between the public and private sectors in protecting information systems supporting critical infrastructure in key economic sectors and providing reports on the issue to the President, as appropriate;
- Enhancing cooperation between the public and private sectors in protecting critical infrastructure assets in other key economic sectors and providing reports on these issues to the President, as appropriate; and
- Proposing and developing ways to encourage private industry to perform periodic risk assessments of critical information and telecommunications systems.

Executive Summary

The National Infrastructure Advisory Council (NIAC) set out to determine whether the right people are receiving the right intelligence information at the right time to support robust protection and resilience of the Nation's critical infrastructure. More than 200 interviews and extensive open-source research uncovered a wealth of insights on this complex problem. First, there have been marked improvements in the sharing of intelligence information within the Federal Intelligence Community, and between the Federal Government and regions, States, and municipalities. However, this level of improvement has not been matched in the sharing of intelligence information between the Federal Government and private sector owners and operators of critical infrastructure. Despite some notable successes, this bi-directional sharing is still relatively immature, leaving a large gap between current practices and an optimal system of effective public-private intelligence information sharing. We observe that trust is the essential glue to make this public-private system work. Trust results when partner capabilities are understood and valued, processes are tailored to leverage these capabilities, and these processes are tested and proven valuable to all partners. When breakdowns in information sharing occur, it erodes trust and is counterproductive to risk management.

Information sharing is perhaps the most important factor in the protection and resilience of critical infrastructure. Information on threats to infrastructure and their likely impact underlies nearly every security decision made by owners and operators, including which assets to protect, how to make operations more resilient, how to plan for potential disasters, when to ramp up to higher levels of security, and how to respond in the immediate aftermath of a disaster. We looked at intelligence information flowing from the Federal Government to critical infrastructure owners and operators as well as risk information flowing from critical infrastructure owners and operators to the government. Our study reveals the complex ways information is gathered, analyzed, packaged, and shared among the owners and operators of critical infrastructures.

In tackling this complex subject, we examined the different stages of the intelligence cycle, including requirements generation, information collection, analysis, and dissemination. To gather a variety of perspectives, we conducted extensive interviews with security directors, chief executives, subject matter experts, and government executives and managers. Recognizing that distinct sector characteristics shape information sharing needs, we conducted case studies of five sectors: Commercial Facilities, Healthcare and Public Health, Energy (Oil and Natural Gas), Banking and Finance, and Chemical. While we found some information sharing approaches to be effective, others were not. As a result, we adopted a "capability maturity approach," which acknowledges that different Federal agencies have different abilities to share information effectively, and we sought to build on what is working.

The NIAC's Task

The Administration requested that the NIAC examine three specific topics in this study:

- Review the overall progress and status of bi-directional intelligence information sharing.
- Examine ways to improve the private sector role in counterintelligence.
- Assess the role of fusion centers as a mechanism for sharing intelligence information with the private sector.

We interpreted the request to examine "counterintelligence" to mean "counterterrorism." The distinction matters—both in how the Federal Intelligence Community and private sector define the term and their roles surrounding it—and is explained further within the report.

The Nation’s Intelligence Information Sharing Challenge

The Council discovered a complex knot of attitudes and structural issues that work against information sharing. We discovered benefits to the Nation that could be realized if we have the will to more effectively leverage the knowledge and insights of the owners of critical infrastructure. The Council believes that if properly managed, information sharing between the public and private sectors could be one of our most powerful tools to combat terrorism, natural disasters, and criminal activity.

The Council has developed detailed findings and corresponding recommendations to improve bi-directional information sharing. The following overarching observations provide context that underlies all of our findings and recommendations.

1. **The public-private sector component of the infrastructure protection mission is not receiving the high priority that is commensurate with its vital importance to the Nation’s economic health and security.** While the Federal Intelligence Community serves multiple customers and missions, sharing information with the owners and operators of critical infrastructure does not receive high priority, either in the Department of Homeland Security (DHS), the Federal Intelligence Community at large, or Federal and State governments.
2. **The unique knowledge and analysis capabilities offered by the private sector are not widely understood by government, and where they are understood, the processes to leverage these capabilities are not in place.** The Federal Intelligence Community has not tapped into the full capability set of the private sector, which can provide the context to identify and assess critical information, help analyze complex problems, and anticipate and develop solutions to reduce risks.
3. **Public and private sector incentives for sharing information are not aligned to serve the infrastructure protection mission.** The Federal Intelligence Community typically shares information on a “need-to-know” basis. The private sector, by contrast, has moved toward providing information on a “need-to-share” basis. It appears that possible penalties for sharing information more widely within the Federal Intelligence Community may often outweigh likely payoffs. The result is conflicting value propositions that affect fundamental decisions about what and how information is shared. However, if private sector information can be used to inform Federal intelligence, this can usefully change the Federal value proposition.
4. **The Federal intelligence sharing enterprise is complex and often confusing.** While having a single point of contact for sharing with the Federal Intelligence Community is not optimal, *simplification and clarity* is needed. Today, the multiplicity of Federal players, their diverse missions and roles, and myriad “rules-of-the-road” for how and where intelligence can be shared, stymie owners and operators of critical infrastructure in their ability to contribute to and use intelligence information. As a result, engagement through trusted personal relationships remains a primary means of facilitating the flow of needed intelligence information.
5. **The Department of Homeland Security is not serving as an effective champion and leader for the intelligence information sharing interests of the private sector in the overall infrastructure protection mission within the Federal Intelligence Community and other government agencies.** The Department has special linkages with private sector owners and operators that could be leveraged to provide a unique and important source of information for the Federal Intelligence Community while enhancing private sector engagement.

These issues must be addressed head on if we are to build trusted and efficient information flows between the public and private sectors and reduce risks to the Nation's critical infrastructure. Our specific findings and recommendations are summarized below and fully described in the body of this report.

Findings

While intelligence information sharing has improved since the Council's 2006 report on *Private-Public Intelligence Sharing,* the present state is not sufficient to maximize the protection and resilience of the Nation's infrastructure. The NIAC observes that in the past five years there have been important advances in intelligence sharing. Specifically, (1) the Federal Intelligence Community, through the leadership of the Director of National Intelligence, appears to have coalesced to improve information sharing among Federal agencies and (2) DHS information sharing with regions, States, and municipalities has improved through mechanisms such as fusion centers. In contrast, bi-directional sharing with private sector owners and operators of critical infrastructure is less developed and successes are harder to come by, with a few notable exceptions.

The Council reaffirms a finding from our 2008 study, *Critical Infrastructure Partnership Strategic Assessment*: the voluntary public-private partnership is the best long-term strategy to secure our critical infrastructures. We recognize that regulations and standards, if developed wisely with the full collaboration of the regulated private sector entities, have their place in protecting critical infrastructures. However, we consider a non-regulatory approach, which encourages industry and government to diligently pursue common national infrastructure protection goals while avoiding unnecessary costs and inefficiencies, to be the preferred approach and in the best interests of the Nation. This fundamental belief underlies our approach on how to improve information sharing.

Although the private sector has not been a traditional partner or customer of the Federal Intelligence Community, Federal law and policy clearly make critical infrastructure private sector owners and operators one of today's customers. However, actual implementation lags this authority. The critical infrastructure imperative is widely recognized; for three years in a row (2009–2011) a Presidential Proclamation has designated December as "Critical Infrastructure Protection Month." **Still, we find that the priority of information sharing with critical infrastructure owners and operators, both within parts of DHS and across the Federal Intelligence Community as a whole, does not appear to be commensurate with the widely acknowledged importance of critical infrastructure to the Nation's economic strength and our citizen's way of life.**

Our specific findings are summarized in Figure ES-1, organized by seven topics.

- **Authority and Policy:** Is the appropriate authority and policy structure in place, and is it clear and understood by all partners?
- **Implementation of Authority:** Do the organizational structures and processes enable effective integration of threat, vulnerability, and consequence information within and across public and private sector partners?
- **Capability Leveraging:** Do the Federal Intelligence Community and the private sector understand and leverage each other's capabilities?
- **Information Content:** Is there a bi-directional flow of products, with Federal products that meet sector requirements, and private-sector products that meet Federal requirements?

- **Information Delivery:** Are there effective bi-directional processes that enable the timely sharing of information between the Federal Intelligence Community and the private sector?
- **Counterintelligence/counterterrorism:** What information and capability can the private sector contribute to provide solutions in protecting the Nation's infrastructure?
- **Fusion Centers:** What is the effectiveness of the fusion center model in meeting the needs of private-sector critical infrastructure owners and operators?

Figure ES-1: Findings

Findings
1. Authority & Policy
A. Federal law and policy clearly include the private sector as a customer of the Federal Intelligence Community. B. DHS has clear authority to share with the private sector the counterterrorism and critical infrastructure protection information developed by the Federal Intelligence Community. C. The priority of critical infrastructure protection, both within parts of DHS and the Federal Government at large, appears to be low and is not commensurate with the important role of critical infrastructure in the Nation's security and economy. D. There is currently not an effective process to engage—in a systematic and *sustained* manner—senior executives in the private sector with their counterparts in government.
2. Implementation of Authority
A. DHS's implementation of its authority within the Federal Intelligence Community for information sharing with private sector owners and operators is uneven, reflecting an early stage of maturity in an evolving model for information sharing. For the Federal Intelligence Community at large, information sharing with owners and operators appears to be similarly constrained, in this case by unfamiliarity with the private sector as a customer. Even where understanding is good, processes remain deficient. B. The Federal Intelligence Community often does not understand what information the private sector needs, nor does the private sector always understand the actual capabilities and missions of the Intelligence Community. C. The separation of the original DHS Directorate for Information Analysis and Infrastructure Protection into two separate organizations appears to have adversely affected the sharing and fusing of intelligence information in overall public-private risk-management processes. D. The complexity of roles and responsibilities in the Federal intelligence-sharing enterprise is confusing to the private sector, and it lacks the clarity needed to be truly effective.
3. Leveraging the Capability of the Private Sector to Reduce Risk
A. The unique knowledge and analysis capabilities offered by the private sector are not widely understood by government, and where they are understood, the processes to leverage this capability are not in place. B. Differing incentives and disincentives, within and across the Federal Intelligence Community and the private sector, make a shared value proposition that encourages information sharing difficult to define and achieve. C. Intelligence information-sharing mechanisms between the private sector and the Federal Government are complicated, at times confusing to the private sector, and may be redundant and/or conflicting. As a result, engagement through trusted personal relationships remains a primary means of facilitating the flow of needed intelligence information. D. The private sector is willing and able to share information with government that may be useful in counterterrorism efforts. However, the private sector perceives that the government is not yet prepared

Findings

to receive information from the private sector, to act on it, or to provide feedback on whether the information was investigated and found to be useful.

E. There are emerging models of successful bi-directional intelligence information sharing, including the engagement process used by some Sector-Specific Agencies (SSAs) and three DHS pilot efforts: 1) the Classified CIKR Engagement Working Group, 2) HITRAC Classified Information “Reading Room,” and 3) an effort with the Banking and Finance Sector to define intelligence-sharing protocols.

F. There are also models of success for Sector Coordinating Councils (SCCs); these should provide lessons for successful engagement with owners and operators, starting with the fundamental need to define and inform the companion SSA on sector intelligence needs.

4. Information Content

A. The private sector generally does not receive the intelligence information it needs, though this varies somewhat across sectors. With the exception of asset-specific threats, the majority of information received is reactive to events rather than usefully predictive.

B. In addition to finished intelligence products, fragmentary information is highly valuable to the private sector, particularly given the need for timely information. Information otherwise viewed as fragmentary or not relevant by the Federal Intelligence Community may in fact be highly relevant within the context of sector operations.

C. Nearly 10 years after 9/11, the DHS Office of Intelligence and Analysis is now developing a pilot program, the Sector Information Needs process, to engage the private sector in defining owner/operator requirements.

D. DHS is in the nascent stages of using predictive analytics. In comparison, other components of the Federal Intelligence Community and the private sector already make effective use of these tools. DHS should leverage this powerful, state-of-the-art approach to provide timely threat analysis and warning.

5. Information Delivery

A. Intelligence sharing processes, tools, and products are improving but need to be significantly better. This includes, for example, improved classified and unclassified briefings and timely delivery of information useful for prevention and risk mitigation.

B. Currently, the use—and usefulness—of the Homeland Security Information Network – Critical Sectors (HSIN-CS) as a preferred mechanism for sharing is modest at best. On the whole, HSIN-CS does not meet the requirements of private sector owners and operators, and its technology platform does not take advantage of current, off-the-shelf tools that can significantly contribute to meeting the time-critical needs of threat analysis. However, the recent DHS business-case assessment for HSIN acknowledges these deficiencies and is driving plans to remediate them.

C. The private sector reaches out to multiple sources to meet its intelligence needs, including trusted personal relationships, trade associations, various DHS components, other government agencies such as the FBI, Sector Specific Agencies, sector Information Sharing and Analysis Centers, fusion centers, and State and local law enforcement. While it is important to note that the “value proposition” of various sources and mechanisms varies across sectors, there is a common concern over receiving redundant, late, or conflicting information.

D. The Critical Infrastructure Partnership Advisory Council (CIPAC) structure—and its constituent members, which include owners and operators that are members of their respective Sector Coordinating Council and their representative trade or equivalent organizations—is an essential foundation for effective information sharing. As part of this foundation, trade associations play an essential role in information sharing. For example, they may be the only formal information sharing mechanism for small and medium-sized businesses.

Findings
6. Counterintelligence/Counterterrorism
A. "Counterintelligence" has specialized meaning in the Intelligence Community that is largely outside of the realm of the private sector. The term "counterterrorism information" more accurately describes the information the private sector is attuned to and to which it can contribute. B. The private sector has knowledge and capabilities that can help anticipate and solve problems. Providing data is only one capability; the sectors can provide context and contribute to analysis that drives data needs.
7. Fusion Centers
A. The fusion center model appears to be effective for law enforcement and first-responder engagement with State, regional, and local communities. The use of fusion centers for sharing intelligence information with the private sector varies dramatically across locations and sectors, but overall seems comparatively modest. There are, however, several good models of success in this regard.

While this study is directed to sharing with private-sector owners and operators, some sectors have significant numbers of public-sector owners and operators. We believe these findings and the recommendations that follow may also apply to these Federal, State, and municipal owners and operators.

Recommendations

The overarching recommendation of the NIAC is that **the Administration should clearly and strongly assert the role and priority of critical infrastructure protection and resilience to national security, economic growth, and the well being of our citizens.** This is particularly important in light of emerging cyber risks, the growing sector interdependencies that affect business continuity, and ongoing criminal or terrorist threats to the Nation. Without this foundation, it will be hard to accelerate the adoption of an effective bi-directional process of engagement that leverages the full capabilities of public and private partners across the entire intelligence cycle. There are seven areas of recommendations—five for the overall intelligence information sharing process and one each for counterterrorism and fusion centers—that address the critical role of bi-directional information sharing in achieving the shared mission of infrastructure protection and resilience. The recommendations are presented in Figure ES-2.

Figure ES-2: Recommendations

Topics	Recommendations
1. Assert the Priority of Infrastructure Protection and Resilience in National Security	While the White House clearly recognizes the critical infrastructure protection imperative, it should vigorously affirm the criticality of infrastructure protection and resilience to our Nations’ security and our citizen’s well being through policy emphasis that drives action. Through a Presidential Policy Directive or other policy mechanism, the White House should direct DHS and the Intelligence Community to: weigh issues of harm to critical sectors against other missions in all operations, collect infrastructure intelligence needs and evaluate terrorist targets in the critical sectors, and prepare a quadrennial report on infrastructure protection intelligence sharing. The White House should additionally employ current or new partnership mechanisms for senior executives in the private sector to engage their government counterparts to facilitate a truly National approach that *leverages public-private resources* for large-scale, persistent threats.

Topics	Recommendations
2. Improve the Implementation and Accountability of Existing Authorities	To improve performance and accountability and help mature DHS's role as a member of the Federal Intelligence Community, the NIAC recommends: a. The Office of the Director of National Intelligence (ODNI) assist DHS in developing, modifying, or assessing programs and processes for private sector information sharing. b. DHS reexamine the effectiveness of its risk management organizational structure, specifically the separation of threat analysis (in the Office of Intelligence and Analysis) from vulnerability and consequence analysis (in the Office of Infrastructure Protection). c. DHS, supported by ODNI, establish core teams of 3-4 intelligence specialists specifically for each sector, and one team focused on cross-sector information issues. d. ODNI aim to reduce ambiguity and simplify engagement points and processes in the rules and relationships for information sharing. e. The President define the functions (and authority to execute them), expected outcomes, and accountability measures for Sector-Specific Agencies (SSAs).
3. Improve Information Content by Leveraging Partner Capabilities	To ensure that the Federal Government and the private sector can work effectively as partners in intelligence requirements definition, collection, analysis, and dissemination, the NIAC recommends that DHS work with each Sector-Specific Agency to implement, for all 18 critical infrastructure sectors, a robust intelligence requirements process that 1) meets the information needs of owners and operators, 2) delivers these requirements to appropriate elements of the Federal Intelligence Community, 3) is consistent with existing Intelligence Community processes, and 4) supports advocacy for critical infrastructure priority within the Intelligence Community. To support these requirements, the NIAC recommends that DHS develop a more robust and timely analysis capability that leverages knowledgeable personnel and enhanced analytical resources for each critical infrastructure sector, to support sector-specific needs, business models, and risk-management processes. DHS should leverage commercially-available tools and techniques to provide capabilities for predictive intelligence for critical infrastructure protection.
4. Improve the Value of Information Products to Industry Risk-Management Practices	To ensure that the types of intelligence information used for protection and resilience are shared among partners, the NIAC recommends that the Office of the Director of National Intelligence (ODNI), working jointly with DHS, establish new intelligence dissemination product formats to create tailored and practical products that help owners and operators protect assets and improve business continuity. DHS and its Federal intelligence partners should supplement classified threat briefings with unclassified reports that can be readily and broadly shared.

Topics	Recommendations
5. Build Accepted Practices for Timely Information Delivery	All Federal mechanisms for sharing intelligence information should be examined with the goal of simplifying pathways, eliminating redundancy, and ensuring consistency of the information delivered. DHS should collaborate with the private sector to 1) identify critical infrastructure intelligence information sharing pathways and 2) establish sector-specific intelligence information sharing protocols with the specific goal of improving timeliness. DHS and the Sector-Specific Agencies should work with the Sector Coordinating Councils to create formal networks of private-sector chief security officers and site security managers that will be used to facilitate timely, bi-directional public-private intelligence information sharing. DHS should guide Homeland Security Information Network – Critical Sectors (HSIN-CS) implementation to achieve three desired outcomes: 1) sectors are better educated that they *are the customer* and their needs drive system requirements, 2) system implementation is based on and measured by *understanding and meeting these user needs*, and 3) system architecture takes advantage of state-of-the-art, commercially available tools for threat analysis in order to meet these needs in a timely manner. Appropriate senior-level management leadership and oversight must be provided to keep this goal on track.
6. Capitalize on Private Sector Capabilities for Counterterrorism Solutions	The Federal Government should capitalize on the information collection and analysis capabilities of private-sector partners, and incorporate this knowledge base to improve existing products and processes. DHS should provide specific guidance on the most important areas of emerging counterterrorism information on which the sectors should focus, and update these areas on a regular basis as conditions dictate.
7. Enhance Fusion Center Capabilities as One Mechanism for Sharing	Where appropriate, DHS should guide fusion centers to establish an information sharing function with owners and operators as part of a critical infrastructure protection and resilience mission. We recognize that not all fusion centers align with critical infrastructure assets, or operate under State laws and policy that allow or encourage the integration of critical infrastructure information. Regardless, DHS should support—through funding, personnel, training, technology, and analytic tools—the development of an infrastructure protection and resilience capability that could stand alone or be integrated within fusion centers to facilitate the flow of intelligence information to and from the private sector, while ensuring information protection and addressing privacy concerns. Where this mission alignment with fusion centers does not take place, DHS should instead direct available critical infrastructure protection resources to an alternative approach *specifically designed with information sharing with private sector owners and operators as its goal.* If a grant process is used for fusion centers, it should specifically require an infrastructure protection mission and a process for sharing with the private sector.

1.0 Study Overview: Challenges and Approach

Effective critical infrastructure protection and resilience relies on access to timely, accurate, and actionable information. Reliable information on suspected threats, known vulnerabilities, and their potential consequences enables infrastructure owners and operators to assess risks and take action, such as prioritizing assets, implementing effective security measures, and improving emergency plans. Such information underlies nearly every security decision, and the most valuable threat information that the private sector receives originates in the government. From the ground up, information on threats or suspicious activity observed by owners and operators at the asset level can give insight into potential national-level threats. **Simply put, the public and private sectors each hold valuable information that can help the other reduce risks to critical infrastructures.**

Legislation enacted since 2002 explicitly recognizes critical infrastructure owners and operators as legitimate customers of classified and unclassified government intelligence information. In the last decade, laws and policy changes have helped to build a new model of bi-directional intelligence information sharing by formally fostering government and private sector relationships. This study examines the maturity of information sharing between government intelligence agencies and critical infrastructure owners and operators.

The NIAC Mission

The NIAC provides the President of the United States with advice on the security of physical and cyber infrastructure supporting critical sectors of the economy. It also has the authority to provide advice directly to the heads of other agencies that have shared responsibility for critical infrastructure protection, such as Health and Human Services, Transportation, and Energy. The NIAC is charged with improving public-private cooperation and partnership in securing critical infrastructure by advising on policies and strategies that bolster risk assessment and management, information sharing, protective strategies, and clarified roles and responsibilities between public and private sectors.

The NIAC was created by Executive Order 13231 of October 16, 2001, as amended by Executive Order 13286 of February 28, 2003, Executive Order 13385 of September 29, 2005, and Executive Order 13585 of September 30, 2011. The Council is composed of not more than 30 members, appointed by the President, who are selected from the private sector, academia, and State and local government, representing senior executive leadership expertise from the critical infrastructure and key resource sectors as defined in Homeland Security Presidential Directive-7 (HSPD-7).

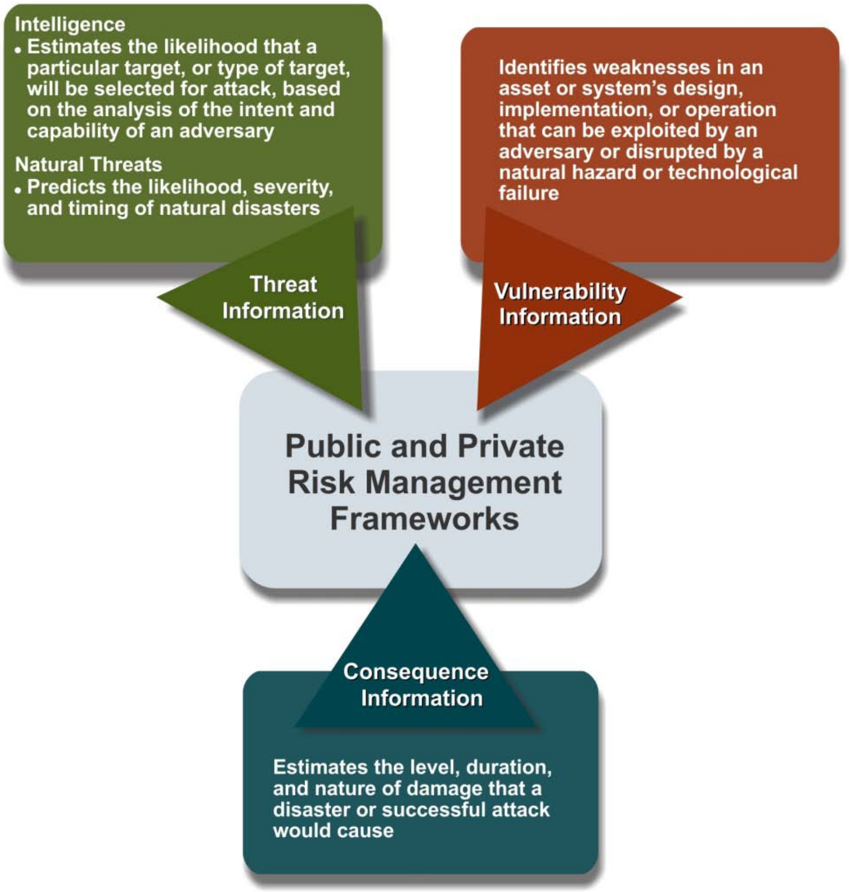
Charge to the National Infrastructure Advisory Council (NIAC)

The sharing of intelligence information was the primary focus of the Council's 2006 study on *Public-Private Sector Intelligence Coordination* and has been frequently mentioned in other NIAC studies. In 2010, the Administration requested that we revisit this study to examine three specific aspects of intelligence information sharing:

- Review the overall progress and status of intelligence information sharing since the NIAC's 2006 study, addressing 1) the timeliness and relevance of information and intelligence shared between the public and private sectors and 2) the effectiveness of bi-directional processes and products for sharing between government and the private sector.
- Examine ways to enhance owner and operator contributions to counterintelligence, addressing 1) the private sector role in counterintelligence and 2) challenges and potential solutions to improving contributions by owners and operators.
- Assess the role of fusion centers as a mechanism for sharing intelligence information with the private sector, addressing 1) private sector participation and interaction and 2) information sharing challenges, gaps, and best practices.

1.1 The Challenge of Sharing Intelligence in Complex Systems

Figure 1-1. Intelligence Information as a Component of Risk-Management

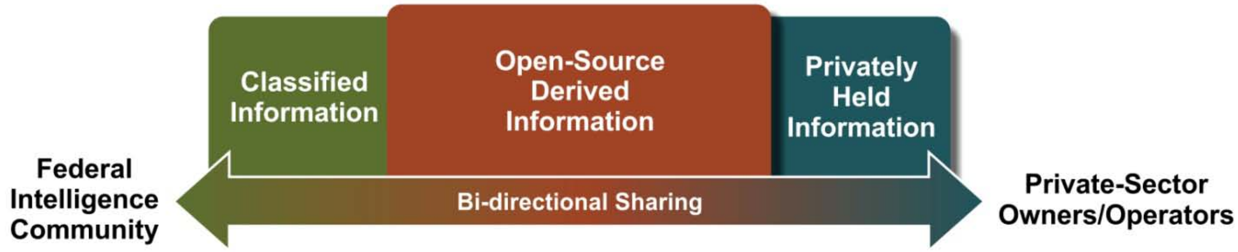

Intelligence
• Estimates the likelihood that a particular target, or type of target, will be selected for attack, based on the analysis of the intent and capability of an adversary
Natural Threats
• Predicts the likelihood, severity, and timing of natural disasters
Threat Information
Identifies weaknesses in an asset or system's design, implementation, or operation that can be exploited by an adversary or disrupted by a natural hazard or technological failure
Vulnerability Information
Public and Private Risk Management Frameworks
Consequence Information
Estimates the level, duration, and nature of damage that a disaster or successful attack would cause

The public and private sectors share the goal of critical infrastructure protection and resilience, which is implemented through an array of risk-management processes - some private, some public, and some shared. It is important to frame the role of intelligence sharing in risk management, which integrates information on threat, vulnerability, and consequence to evaluate risk –to the Nation as a whole, to a sector, or to a specific asset. Figure 1-1 shows the three elements of risk-management, as well as showing the two primary components of threat information: intelligence information on intentional man-made threats and information on threats from natural causes. As risk is calculated through the synthesis of threat, vulnerability, and consequence information, each element alone is simply one piece of an incomplete puzzle.

Sharing information between the government and the private sector is a balance of interests. As noted, both the public sector and the private sector have a vested interest in effective risk management. The government needs to protect national interests, and risk management is an essential part of business survival. From a business perspective, surviving a terrorist threat is no less important than surviving a market shift. The private and public missions and operating cultures, however, are fundamentally different. The Federal Intelligence Community (IC) is charged with collecting and analyzing extremely sensitive information on National security and shares on a "need to know" basis—sharing only with those who must be informed to meet IC missions and keeping information within protected circles. The private sector, by contrast, operates more on a "need to share" basis—generally withholding only that required to protect privacy and business competitiveness. Neither model, however, encourages a free flow of information to a wide range of stakeholders.

Accordingly, intelligence information sharing is rarely simple. The government is charged with guiding national programs for critical infrastructure protection across 18 critical infrastructure sectors, each with distinct assets, risk profiles, business structures, and regulatory structures. These circumstances shape each sector's information needs and create a complex network of relationships and information sharing mechanisms that must be navigated. Yet government and industry can both bring valuable capabilities to bear. As shown in Figure 1-2, the Federal Government provides classified threat information, the private sector provides suspicious activity and privately held threat and vulnerability information, and both draw upon open sources of information. The most effective bi-directional sharing occurs when each stakeholder leverages their own information against that provided by others to create a clearer picture of the threat environment and support better-informed risk analysis and risk mitigation.

Figure 1-2. Bi-Direction Exchange of Intelligence Information between the Public and Private Sectors


Classified Information
Open-Source Derived Information
Privately Held Information
Federal Intelligence Community
Bi-directional Sharing
Private-Sector Owners/Operators

Bi-directional sharing of capabilities across the full intelligence cycle of requirements, collection, analysis, and dissemination is a relatively new and evolving model of intelligence information sharing. While the Federal Intelligence Community traditionally provides classified threat information, and the private sector may provide information on suspicious activities, these efforts are not part of a broad, bi-directional engagement that leverages the full capabilities of each partner. Several factors underlie this challenge:

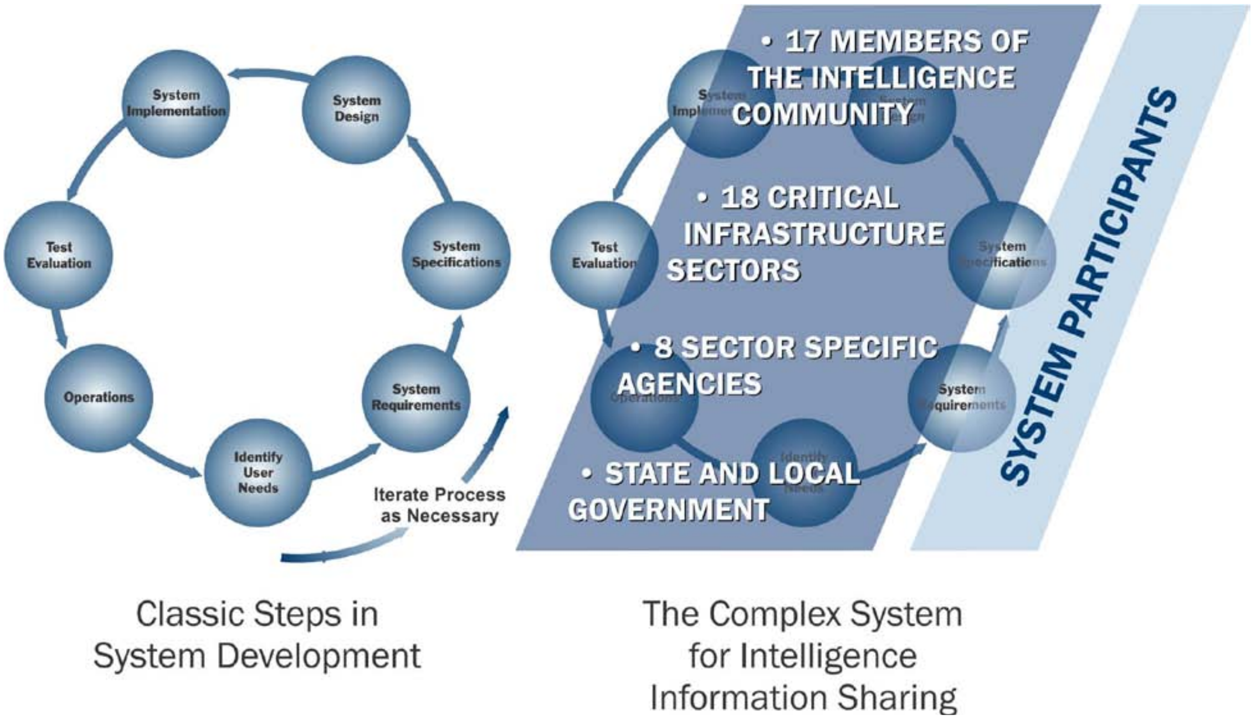
- The private sector is a relatively new partner and customer of the Federal Intelligence Community, at a time when the demands of traditional missions—including military force support and law enforcement—remain high.
- While traditional Federal intelligence processes focus on classified sources and products, *non-classified information held by the private sector* is an emerging contributor to the understanding of threats to our Nation.
- *Open-source information and analysis* is a growing portion of the flow of threat information, and broadly integrating this flow from multiple sources is a new requirement.
- Challenges in sharing classified information with the private sector have less to do with the classification level of the information, and more with the *confusing policies and processes for sharing classified information.*
- Finally, sharing intelligence in this model means that trusted *organizational, functional, and personal* relationships must be developed and tested. In virtually every NIAC study to date, the importance of trusted relationships has been underscored.

Although this new paradigm is challenging, it is not an indictment of the systems in place today. It simply recognizes that it takes time, dedication, and resourcefulness to bring a system to maturity.

1.2 Study Approach

Given this paradigm, our study applied a “capability maturity model” approach, which examines how far systems and processes have progressed toward full capability of an ideal, mature system. In doing so, we examined bi-directional information sharing as a complex “ecosystem” of participants encompassing an array of public and private partners: 18 critical sectors, 17 members of the Federal Intelligence Community, 8 Sector-Specific Agencies, 72 State and regional fusion centers, and other participants. We used the classic development process for information systems as a model, as shown in Figure 1-3. While this process is typically used in physical/cyber systems for information management, it is a useful paradigm for examining the broader challenge. This model recognizes that complex systems often take multiple cycles of a system-development process to reach the desired level of performance.

Figure 1-3. The Challenge of Aligning Needs and Capabilities in Complex Systems


System Implementation
System Design
Test Evaluation
System Specifications
Operations
System Requirements
Identify User Needs
Iterate Process as Necessary
• 17 MEMBERS OF THE INTELLIGENCE COMMUNITY
• 18 CRITICAL INFRASTRUCTURE SECTORS
• 8 SECTOR SPECIFIC AGENCIES
• STATE AND LOCAL GOVERNMENT
SYSTEM PARTICIPANTS
Classic Steps in System Development
The Complex System for Intelligence Information Sharing

To achieve the shared mission of infrastructure protection and resilience, the ideal system for bi-directional information sharing would have the following characteristics:

- Infrastructure owners and operators are a valued and trusted partner of the Federal Intelligence Community.
- The intelligence information requirements of the infrastructure sectors, along with the operational context for these requirements, are understood by the Federal Intelligence Community.
- Intelligence information sharing is an integrated part of overall public-private information sharing structures and processes, such that threat, vulnerability, and consequence information are routinely fused to provide useful products for risk management.
- The capabilities of the private sector—to provide data, context, and analysis—are understood and integrated into a *national* capability for intelligence information that includes the private sector, the Federal Intelligence Community, and State and local partners.

The findings and recommendations within this report are specifically aimed at maturing this model to enable public and private partners to better leverage distinctive capabilities and address risks in an all-hazards environment.

The study examined the different stages of the intelligence cycle, including requirements generation, information collection, analysis, and dissemination. We conducted more than 200 interviews with security directors, chief executives, and subject matter experts, and government executives and managers, to obtain a wide range of expertise in risk management, intelligence, and sector operations. These interviews were augmented with a comprehensive examination of open-source material.

The study benefitted from the experience and knowledge of many individuals - Working Group members, Study Group members, leaders of case studies, and other subject matter experts. We acknowledge these individuals in Appendix A, and are grateful for their expertise, perspective, insight, and dedication.

A recurring theme of NIAC studies is that a "one-size-fits-all" approach does not work well in applying protection and resilience solutions to all 18 critical infrastructure sectors. To fully understand how sector characteristics shape information sharing needs, the NIAC conducted case studies in the following sectors:

- Appendix B: Banking and Financial Services Sector
- Appendix C: Chemical Sector
- Appendix D: Commercial Facilities Sector
- Appendix E: Healthcare and Public Health Sector
- Appendix F: Oil and Natural Gas (Energy Sector)

The case studies identify sector-specific characteristics that shape approaches to intelligence sharing, provide examples of successful bi-directional information sharing and areas for improvement, and include sector-specific findings and conclusions. They also examine the knowledge and use of fusion centers and the sector role in providing counterterrorism information. During the course of this study, we identified numerous other recent studies in which the findings and recommendations align extremely well with those of this study. Appendix G identifies some of these studies.

Section 2 of this report provides necessary background information to understand the policies and processes that have shaped the current context of information sharing. The outcomes of each case study, examined in this context, form the basis of the overall study findings and recommendations provided in Sections 3 and 4. The findings more fully characterize the complex challenges in bi-directional information sharing between the government and private sector, while the recommendations identify specific actions that aim to advance the maturity of the information sharing model.

2.0 Study Context

Federal policy and legislation introduced over the last decade support the paradigm shift to a bi-directional flow of intelligence information between the government and private sector. Most notably, they clearly establish critical infrastructure owners and operators as an important customer of the Federal Intelligence Community and designate the Department of Homeland Security (DHS) as the lead for representing critical infrastructure needs within this community. In conjunction, many of these authorities encourage unprecedented partnership mechanisms among the public and private sectors to support critical infrastructure protection and risk mitigation. Table 2-1 shows the timeline of the assignment and implementation of new authorities since 1998.

Table 2-1. Key Federal Events and Implications for Infrastructure Intelligence Sharing

Year	Event	Impact
1998	Presidential Decision Directive -63 (PDD-63), *Critical Infrastructure Protection*, is released.	PDD-63 establishes the policy framework for protecting critical infrastructure through public-private collaboration, including information sharing.
2001	September 11 attack on the World Trade Center and Pentagon.	Elements of critical Infrastructure are primary targets of the attacks.
2002	Homeland Security Act passed by Congress and signed into law.	DHS is designated as the newest member of the Federal Intelligence Community.
2003	DHS establishes the Directorate for Information Analysis and Infrastructure Protection (IAIP). Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, is released.	The IAIP function covers the threat, vulnerability, and consequence elements of risk management. HSPD-7 establishes Sector Specific Agencies as the Federal coordinating mechanism for infrastructure protection. DHS and seven other agencies are assigned the SSA function.
2004	Intelligence Reform and Terrorism Prevention Act passed, establishing Office of the Director of National Intelligence. DHS establishes the Homeland Security Information Network (HSIN).	Places the 17 elements of the Federal Intelligence Community under ODNI for coordination purposes. HSIN is to serve as primary information-sharing platform for DHS functions.
2005	DHS reorganization, separating IAIP into the standalone Office of Intelligence and Analysis (I&A) and Office of Infrastructure Protection (IP) within the National Protection and Programs Directorate. Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) established.	Separates threat element (now in I&A) from vulnerability and consequence elements (in IP). I&A now has other missions in addition to Infrastructure protection. HITRAC purpose is to integrate intelligence reporting and analysis between I&A and IP.
2006	First version of National Infrastructure Protection Plan (NIPP) published. Critical Infrastructure Partnership Advisory Council (CIPAC) established. Protected Critical Infrastructure Information (PCII) Program introduced.	Establishes the public-private partnership model for infrastructure protection. CIPAC creates Sector Coordinating Council structure to facilitate information sharing. Establishes an information-protection program to shield private sector, voluntarily submitted information from public disclosure.
2007	Critical Infrastructure and Key Resources Information Sharing Environment (CIKR-ISE) incorporated into National ISE as its private sector component.	Provides framework to guide infrastructure information sharing strategic, situational awareness, and operational response levels.
2009	Revised NIPP is released. National Information Sharing Strategy released.	Infrastructure resilience becomes companion focus to protection.
2011	Office of Intelligence and Analysis (I&A) Institutes formal process for intelligence needs identification.	Oil and Natural Gas and Chemical Sectors engaged through pilot programs.

The remainder of this section summarizes the specific authorities and policies that sanction critical infrastructure as a customer of intelligence (2.1), and examines how the private sector operates as both a consumer and provider of intelligence information (2.2).

2.1 Federal Authority and Policy

Authorities

The key authorities for public-private intelligence information sharing are listed in Figure 2-2. These and other authorities clearly identify the private sector as a legitimate consumer of intelligence and give major operational responsibilities to DHS and the Office of the Director of National Intelligence (ODNI)—which oversees the 17 members of the Federal Intelligence Community—to develop mechanisms to effectively share intelligence information with the private sector.

Figure 2-2. Major Authorities for Public-Private Intelligence and Information Sharing

	USA PATRIOT Act of 2001	• Expanded the definition of terrorism to include domestic terrorism, enlarging the number of activities to which the Act's expanded law enforcement powers could be applied. • Title VII specifically addressed increased information sharing for critical infrastructure protection.
Law	**Homeland Security Act of 2002**	• Created Department of Homeland Security. • Required President to implement procedures for Federal agencies to share classified and unclassified homeland security information with appropriate State and local personnel (including private sector entities).
	Intelligence Reform and Terrorism Prevention Act of 2004	• Established Office of the Director of National Intelligence (ODNI) to coordinate intelligence and information sharing within the Federal Government. • Directed President to establish Information Sharing Environment (ISE) with policies and procedures for sharing terrorism information with the private sector.
	Implementing Recommendations of the 9/11 Commission Act of 2007	• Required DHS Secretary to establish department-wide procedures to receive and analyze intelligence from State, local, and tribal authorities, and the private sector. • Specified authorities for DHS Under Secretary for Intelligence and Analysis to integrate and standardize Department intelligence components. • Required DHS Secretary to establish a fusion center initiative and provide intelligence advice and analysis to fusion centers. • Created Interagency Threat Assessment and Coordination Group (ITACG) to set processes to share intelligence information with State and local governments and the private sector within ISE.

Policies

In their Executive Orders, Presidential Directives, Executive Memorandum, and national strategies, Presidents Bill Clinton, George W. Bush, and Barack Obama all affirmed that private sector owners and operators of critical infrastructure are customers of national intelligence. President Clinton in the May 22, 1998 Presidential Decision Directive/NSC-63 stated: "It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[1]

President George W. Bush in Homeland Security Presidential Directive 7 of December 17, 2003, established as U.S. policy: "Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies will work with State and local governments and the private sector to accomplish this objective." HSPD-7 stated that the Secretary of Homeland Security, "consistent with the Homeland Security Act of 2002 and other applicable legal authorities and presidential guidance, shall establish appropriate systems, mechanisms, and procedures to share homeland security information relevant to threats and vulnerabilities in national critical infrastructure and key resources with other Federal departments and agencies, State and local governments, and the private sector in a timely manner."[2]

President Bush further stated in Executive Order 13388 of October 25, 2005:[3]

> Section 1. Policy. To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies:
>
> (a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America; (ii) the interchange of terrorism information among agencies; (iii) **the interchange of terrorism information between agencies and appropriate authorities of State, local, and tribal governments, and between agencies and appropriate private sector entities**; and (iv) the protection of the ability of agencies to acquire additional such information [emphasis added]

As shown in Figure 2-3, the Program Manager of the ISE seated in the ODNI, in its *Information Sharing Environment Implementation Plan*, explicitly aligns with this by recognizing private sector information as a critical element in understanding the threat environment.

In President Barack Obama's 2010 *National Security Strategy*,[4] the merging of National security and homeland security was emphasized as part of a "whole-of-government" approach to strengthening national capability:[5] "We are now moving beyond traditional distinctions between homeland and

[1] Presidential Decision Directive/NSC-63 of May 22, 1998, "Critical Infrastructure Protection," http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[2] Homeland Security Presidential Directive / HSPD-7 of December 17, 2003, "Critical Infrastructure Identification, Prioritization, and Protection," http://www.fas.org/irp/offdocs/nspd/hspd-7.html.

[3] Executive Order 13388 of October 25, 2005, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," http://www.fas.org/irp/offdocs/eo/eo-13388.htm. Related authorities include Executive Orders 13311, 13356, 12333, and 12958, and National Security President Directive 46.

[4] *National Security Strategy*, White House, May 2010, p. 10, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[5] As defined by the Project on National Security Reform (PNSR), whole-of-government is an "approach that fosters government-wide collaboration on purpose, actions, and results in a coherent, combined application of available resources to achieve the desired objective or end state." One of the core reforms recommended by the PNSR was that the Federal Government adopt this approach to address issues that fall outside the normal boundaries of agency responsibilities or which require cross-agency coordination: "Department and agency autonomy must be complemented with the capacity for whole-of-government solutions." See, Project on National Security Reform,

Figure 2-3. The National Information Sharing Environment and the Private Sector

The Program Manager of the Information Sharing Environment (PM-ISE) stated in the 2006 ISE Implementation Plan:

> "**Private sector information** represents a crucial element in both understanding the current threat environment and protecting our Nation's critical infrastructure from targeted attacks. Protecting the interconnected and interdependent U.S. infrastructure also requires a robust public-private partnership that provides the private sector with information on incidents, threats, and vulnerabilities, as well as protects private sector information in such a way that the private sector is willing to share it with government partners. The National Infrastructure Protection Plan (NIPP), released recently by DHS, is the cornerstone document that creates a public-private partnership structure through which to affect a national implementation strategy for HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection….
>
> "An effective framework that ensures a two-way flow of timely, actionable threat information between public and private partners is essential in the War on Terror….The **private sector** owns and operates over eighty percent of the nation's critical infrastructure, and is therefore a primary source and repository for relevant terrorism information." [emphasis added]

Source: Program Manager, *Information Sharing Environment Implementation Plan*, ODNI, November 2006, pp. 19, 75, http://www.ise.gov/sites/default/files/ise-impplan-200611_0.pdf.

national security. National security draws on the strength and resilience of our citizens, communities, and economy. This includes a determination to prevent terrorist attacks against the American people by fully coordinating the actions that we take abroad with the actions and precautions that we take at home. It must also include a commitment to building a more secure and resilient nation, while maintaining open flows of goods and people. We will continue to develop the capacity to address the threats and hazards that confront us, while redeveloping our infrastructure to secure our people and work cooperatively with other nations."

A key element of the whole-of-government approach is for government to partner with the private sector to achieve national goals and objectives. As explained in the *National Security Strategy*:[6] "The ideas, values, energy, creativity, and resilience of our citizens are America's greatest resource…. We must tap the ingenuity outside government through strategic partnerships with the private sector, nongovernmental organizations, foundations, and community-based organizations. Such partnerships are critical to U.S. success at home and abroad, and we will support them through enhanced opportunities for engagement, coordination, transparency, and information sharing."

The Obama administration's *National Security Strategy* stressed the need to integrate "our homeland security efforts seamlessly with other aspects of our national security approach, and strengthening our preparedness and resilience." Ways in which the private sector could participate in this effort include strengthening security and resilience at home and securing cyberspace, as illustrated in Figure 2-4.[7]

Forging a New Shield, November 2008, pp. 383, 551, http://pnsr.org/data/files/pnsr%20forging%20a%20new%20shield.pdf.
The Department of Defense in its 2009 *Quadrennial Roles and Missions Review Report* (QRM) supported the whole-of-government approach in addressing national security challenges. The report said that as part of its vision: "The Department supports institutionalizing whole-of-government approaches to addressing national security challenges. The desired end state is for U.S. Government national security partners to develop plans and conduct operations from a shared perspective." See, QRM, January 2009, p. 31, http://www.defense.gov/news/Jan2009/QRMFinalReport_v26Jan.pdf.

[6] *National Security Strategy* (2010), pp. 15-16.

[7] *National Security Strategy* (2010), pp. 18-19; 27-28.

Figure 2-4. Strengthening Security & Resilience and Securing Cyberspace: The Obama Initiative

Enhance Security at Home by:

- Pursuing initiatives to protect and reduce vulnerabilities in critical infrastructure, at our borders, ports, and airports, and to enhance overall air, maritime, transportation, and space and cyber security
- Developing lines of coordination at home across Federal, State, local, tribal, territorial, nongovernmental, and private sector partners, as well as individuals and communities

Effectively Manage Emergencies by:

- Integrating domestic all-hazards planning at all levels of government and building key capabilities to respond to emergencies
- Continuing to collaborate with communities to ensure preparedness efforts are integrated at all levels of government with the private and nonprofit sectors
- Encouraging domestic regional planning and integrated preparedness programs and encouraging government at all levels to engage in long-term recovery planning
- Continually test and improve plans using exercises that are realistic in scenario and consequences

Improve Resilience Through Increased Public-Private Partnerships by:

- Maintaining critical operations and functions, returning to normal life, and learning from disasters so that their lessons can be translated into pragmatic changes when necessary
- Strengthening public-private partnerships by developing incentives for government and the private sector to:
    - Design structures and systems that can withstand disruptions and mitigate associated consequences
    - Ensure redundant systems where necessary to maintain the ability to operate
    - Decentralize critical operations to reduce vulnerability to single points of disruption
    - Develop and test continuity plans to ensure the ability to restore critical capabilities
    - Invest in improvements and maintenance of existing infrastructure

Secure Cyberspace by:

- Working across the government and with the private sector to design more secure technology that enables better protection and improved resilience of critical government and industry systems and networks
- Continuing to invest in cutting-edge research and development necessary for the innovation and discovery needed to meet cybersecurity challenges
- Strengthening partnerships with the private sector in this vital area
- Working with all key players—including all levels of government and the private sector, nationally and internationally—to investigate cyber intrusion and to ensure an organized and unified response to future cyber incidents

Expanding on this overview of authority and policy, Appendix H reviews the laws, policies, strategies, and implementing structures behind DHS's authority over public-private intelligence and information sharing. The appendix demonstrates that DHS has explicit authority to establish inter-agency procedures for disseminating unclassified and classified homeland security information to the private sector and that the Director of National Intelligence (DNI) has no authority over the direct dissemination of information to private sector entities.

2.2 Critical Infrastructure: Now a Customer and Provider of Intelligence Information

The terms "intelligence," "homeland security information," and "terrorism information" have specific meanings in law, but there is also considerable overlap in the formal definitions. For the purposes of this study, we use the term "intelligence information" to mean information that is not commonly known and that, if acquired by any means, can be analyzed to produce useful or "actionable" products of value to the information consumer. It does not have to come from a specific source or method, or achieve a level of classification, to be considered intelligence. Critical infrastructure owners and operators need intelligence information that provides details they can act on to improve the protection and resilience of their facilities, networks, and systems.

Today's threats blend the interests of National and homeland security necessitating a "whole-of-government" approach to critical infrastructure risk mitigation that recent national strategies and policy recognize. The role of the private sector—which owns and operates the vast majority of the Nation's critical infrastructure—is now being recognized as a critical element to that approach. Though this recognition seems to have developed more rapidly within the private sector than in government, Federal policy makes the private sector a legitimate customer of its intelligence information. None-the-less, as shown in Figure 2-5, such a nontraditional mission challenges the Federal Intelligence Community.

Figure 2-5. The Challenge of Nontraditional Missions

The Project on National Security Reform in its November 2008 report on *Forging a New Shield* stated:

> "[T]he national security system has difficulty fixing responsibility and ensuring accountability for missions no department or agency wants. Usually, such problems arise in what might be referred to as nontraditional mission areas, that is, any missions that are not part of the mainstream core mandate assigned in law to a department or agency. When national security missions do not fall neatly within the bounds of a single organization's core mandate, the system's ability to divide and assign labor often is compromised as strong functional "stovepipes" lead agencies to eschew responsibility for anything that detracts from their core responsibilities. In short, the departments and agencies tend to focus on their core capabilities rather than broader "whole of government" missions or missions that sit on the periphery of an organization's mandated responsibilities. The principal symptom of this problem is the general lack of readiness to conduct nontraditional missions…"

Source: Project on National Security Reform, *Forging a New Shield*, November 2008, p. 196, http://pnsr.org/data/files/pnsr%20forging%20a%20new%20shield.pdf.

Intelligence sources are also changing. The widespread availability of information collection and sophisticated analysis tools are making the private sector a producer of intelligence information as well as the government. The government has begun to recognize benefits to its own intelligence information when it leverages sector-specific capabilities and information available from the private sector.

The Private Sector as a Customer for Intelligence Information

There is no single source of intelligence information for private sector owners and operators of critical infrastructure. Rather, each sector—and individual entities within the sectors—acquires its intelligence from multiple sources, including intelligence agencies or other governmental bodies, open media sources, industry and trade associations, trusted formal and informal networks, and private intelligence organizations. Regardless of the source or classification of the information, the private sector primarily requires information that is applicable to their operations and enables them to take security measures that increase their protection and resilience.

Figure 2-6 provides extensive examples of the kinds of intelligence information the Oil and Natural Gas (ONG) Sector seeks and from which sources.

Figure 2-6. Sources of Intelligence-Derived Information for ONG Sector

Source	Examples
Federal Government	• Classified briefings (regularly scheduled as well as special alerts), normally coordinated and/or conducted by DHS and held in Washington, DC or Houston, TX; often including the FBI • Meetings with TSA on pipeline and transportation issues • Information from the Federal government to the ONG Sector Coordinating Council (SCC); to member trade associations, and to member companies • The U.S. State Department's Overseas Security Advisory Council (mostly for international companies) • The FBI's Domestic Security Alliance Council • Personal contacts within the U.S. Intelligence Community (often because of past employment) • Communication with the ONG Sector Specialist, who is considered especially knowledgeable • DHS organizations such as IP, Office of Intelligence and Analysis (I&A), National Infrastructure Coordinating Center (NICC), and HITRAC • Visits to web-based information sources, such as HSIN-CS, HSIN-ONG, US-CERT, DOE ISERnet, FBI InfraGard, and the NIST Computer Security Resource Center • Collaboration with one or more of the Department of Energy National Laboratories • DHS Daily Infrastructure Reports • Department of Energy data, such as the Energy Assurance Daily Reports
State and Local Governments	• State and local governments • Local law enforcement and mutual assistance groups, including regional response groups • Personal contacts with State Police and Joint Terrorism Task Forces • State and local fusion centers
Private Sector	• Joint briefings and meetings under the Critical Infrastructure Partnership Advisory Council (CIPAC) umbrella between an ONG Working Group and the Chemical Sector • Monitoring current and breaking news through the media, such as CNN • Participation in and close interaction with the ONG SCC and its various working groups, such as the Intelligence Requirements Working Group • Contracted private-sector companies, such as Control Risks Group, ASI Group, Stratfor, and Olive Group, as well as various web-crawling firms • Personal contacts with larger ONG companies with international presence which maintain internal intelligence capabilities • Internal intelligence assets within the company, often staffed by former government intelligence analysts • Participation on security committees (both physical and cyber) within large industry associations, such as the American Gas Association, the National Petrochemical and Refiners Association, the Interstate Natural Gas Association, and the American Petroleum Institute • Frequent discussions with major vendors of cyber software and hardware (especially important for those responsible for IT in ONG companies) • The trade press
International	• Relationships with U.S. and foreign government intelligence agencies (mostly for international companies) • Informal conversations with Army personnel and others stationed in areas of interest to individual companies

Also noteworthy are the many resources offered to the private sector owners and operators of critical infrastructure by DHS and other Sector-Specific Agencies. An extensive annotated list of such resources provided by DHS can be found in the *Private Sector Resources Catalog* published by the DHS Private Sector Office, most recently in July 2011.[8]

[8] See, *Private Sector Resources Catalog*, v. 3.0, DHS Private Sector Office, July 2011, http://www.dhs.gov/xlibrary/assets/pso-private-sector-resource-catalog-3.pdf.

Private Sector Capabilities to Produce Intelligence Information

The private sector has robust capacity to produce intelligence information. It is also generally willing to share this information with government and with other private sector entities, as long as the information is protected from unauthorized disclosure and the companies are not held liable for sharing the information. These are legal hurdles that have not yet been completely resolved, although several mechanisms are in place to protect the interests of the private sector in this regard, including the Protected Critical Infrastructure Information (PCII) program[9] and the Critical Infrastructure Partnership Advisory Council (CIPAC).[10]

Figure 2-7 summarizes the major intelligence information sources the private sector develops and the mechanisms it uses to share that information with public and private information sharing partners.

Figure 2-7. Private Sector Production of Intelligence Information

Information Sharing Partners	Shared Private Sector Intelligence Information and Mechanisms
Government	• Suspicious Activity Reports • Cooperating with multiple government agencies on all aspects of cyber security, including computer network operations, workforce development, education, and awareness programs • Cooperating with multiple government agencies to ensure supply chain continuity both domestically as well as globally • Cooperating with multiple government agencies to protect the U.S. global economic advantage, its trade secrets, and technological know-how, by helping to identify and protect the nation's critical assets and infrastructure • Cooperating with government through research and development in order to anticipate and identify emerging technical threats • Information conveyed during CIPAC briefings and discussions with government officials • Information conveyed during classified or unclassified briefings given by Federal agencies • Meetings with SSAs on sector-specific subjects • Information conveyed to the Federal Government, particularly the GCCs, by the SCCs • Information provided to the Overseas Security Advisory Council and/or the Domestic Security Alliance Council • Information conveyed during personal contacts with U.S. intelligence officials • Information relayed to the Sector Specialist or local PSAs • Information relayed to DHS, including IP, I&A, the NICC, and HITRAC • Information posted on web sites such as HSIN-CS, US-CERT, ISERnet, and InfraGard

[9] The PCII program stemmed from the Critical Infrastructure Information Act of 2002, part of the Homeland Security Act of 2002. PCII is an information-protection program that enhances information sharing between the private sector and the government. If the information submitted satisfies the requirements of the Critical Infrastructure Information Act, it is protected from the Freedom of Information Act, State and local disclosure laws, and use in civil litigation. The rules governing the PCII program can be found in Department of Homeland Security, "6 CFR Part 29 Procedures for Handling Critical Infrastructure Information: Final Rule," Federal Register, Vol. 71, No. 170, September 1, 2006, pp. 52262 – 52277, http://www.dhs.gov/xlibrary/assets/pcii_final_rule_federal_register9-1-06-2.pdf. A description of the PCII program can be found on its DHS-hosted Web site at http://www.dhs.gov/files/programs/editorial_0404.shtm.

[10] CIPAC is a federal advisory committee established by the Secretary of Homeland Security under Section 201 of the Homeland Security Act. The purpose of CIPAC is to facilitate strategic planning and effective discussion of critical infrastructure issues in an environment protected from public disclosure. CIPAC is part of the sector partnership model set up by the National Infrastructure Protection Plan. CIPAC is discussed more fully in Section 2.3 of this report. Also see the DHS-maintained CIPAC Web site at http://www.dhs.gov/files/committees/editorial_0843.shtm.

Information Sharing Partners	Shared Private Sector Intelligence Information and Mechanisms
	• Information shared with the National Laboratories • Information shared with State and local governments, including regulatory agencies, local law enforcement, regional response groups, and fusion centers • Information relayed during personal contacts with State police and Joint Terrorism Task Forces • Information passed on to U.S. intelligence or military from companies with international presence • Analysis generated by company internal intelligence assets • Sharing of insights from discussions with major vendors of cyber software and hardware • Relationships with U.S. and foreign government intelligence agencies (mostly for international companies)
Private Sector	• Networking within industry to encourage cooperation with government to identify foreign intelligence activities and defend national security • Sharing Suspicious Activity Reports with sector members • Discussions during CIPAC meetings • Cross-sector discussions and briefings with government officials • Sector meetings with SSAs on sector-specific issues • Information conveyed during to trade associations meetings • Discussions at SCC meetings • Information provided to OSAC and DSAC with instructions to share with other companies • Insights gained in personal contact within the U.S. Intelligence Community • Information given to Sector Specialists and PSAs, with instructions to share with other companies • Information shared with DHS with instructions to share publically or with sector companies • Postings to web-based information sources, such as HSIN-CS sector portals, US-CERT, ISERnet, and InfraGard • Joint industrial collaboration with the National Laboratories • Submissions to DHS Daily Infrastructure Reports and other similar SSA reports • Cross-sector collaboration with State and local governments, including law enforcement, emergency management, and fusion centers • Collaboration in local Joint Terrorism Task Forces • Monitoring and sharing breaking news through the media • Participation in SCC activities and joint Working Groups • Information provided by contracted private-sector companies, such as Control Risks Group, ASI Group, Stratfor, and Olive Group, as well as various web-crawling firms • Information shared from larger companies with international presence • Information shared from Internal intelligence assets within companies • Participation in security committees within large industry associations • Information shared from discussions with major vendors of cyber software and hardware • Information posted in the trade press • Information gleaned and shared from contacts with U.S. and foreign government intelligence agencies and military personnel

3.0 Findings

3.1 Five Concerns about Current Public-Private Information Sharing

The Council strongly believes that the government is missing an opportunity to better leverage the capabilities and resources of private sector owners and operators to reduce risks to critical infrastructures. To meet this challenge, however, significant improvement will be needed on how intelligence information is identified, developed, and shared among public and private partners.

The Council believes that the voluntary public-private partnership is the best long-term strategy to secure our critical infrastructures. We recognize that regulations and standards, if developed wisely with the full collaboration of the regulated private sector entities, have their place in protecting critical infrastructures. However, we consider a non-regulatory approach, which encourages industry and government to diligently pursue common national infrastructure protection goals while avoiding unnecessary costs and inefficiencies, to be the preferred approach and in the best interests of the Nation. These two modes—regulatory and voluntary—can complicate information sharing between the Federal Government and owners and operators of critical infrastructures. However, we feel that a voluntary process, with appropriate checks and balances, must be the foundation for effective information sharing.

The Council has five concerns that frame our specific findings and recommendations.

1. **The public-private sector component of the infrastructure protection mission is not receiving the high priority that is commensurate with its vital importance to the Nation's economic health and security.** While the Federal Intelligence Community serves multiple customers and missions, sharing information with the owners and operators of critical infrastructure does not receive high priority, either in the Department of Homeland Security (DHS), the Federal Intelligence Community at large, or Federal and State governments.
2. **The unique knowledge and analysis capabilities offered by the private sector are not widely understood by government, and where they are understood, the processes to leverage these capabilities are not in place.** The Federal Intelligence Community has not tapped into the full capability set of the private sector, which can provide the context to identify and assess critical information, help analyze complex problems, and anticipate and develop solutions to reduce risks.
3. **Public and private sector incentives for sharing information are not aligned to serve the infrastructure protection mission.** The Federal Intelligence Community typically shares information on a "need-to-know" basis. The private sector, by contrast, has moved toward providing information on a "need-to-share" basis. It appears that possible penalties for sharing information more widely within the Federal Intelligence Community may often outweigh likely payoffs. The result is conflicting value propositions that affect fundamental decisions about what and how information is shared. However, if private sector information can be used to inform Federal intelligence, this can usefully change the Federal value proposition.
4. **The Federal intelligence sharing enterprise is complex and often confusing.** While having a single point of contact for sharing with the Federal Intelligence Community is not optimal, *simplification and clarity is* needed. Today, the multiplicity of Federal players, their diverse missions and roles, and myriad "rules-of-the-road" for how and where intelligence can be shared, stymie owners and operators of critical infrastructure in their ability to contribute to and use intelligence information. As a result, engagement through trusted personal relationships remains a primary means of facilitating the flow of needed intelligence information.

5. **The Department of Homeland Security is not serving as an effective champion and leader for the intelligence information sharing interests of the private sector in the overall infrastructure protection mission within the Federal Intelligence Community and other government agencies.** The Department has special linkages with private sector owners and operators that could be leveraged to provide a unique and important source of information for the Federal Intelligence Community while enhancing private sector engagement.

3.2 Specific Findings

The Administration requested that the Council examine three topics: (1) the overall progress and status of intelligence information sharing between government and the private sector; (2) ways to improve counterintelligence information sharing between the public and private sectors (based on initial findings, this subsequently focused on the sharing of counterterrorism information); and (3) the role of fusion centers as a mechanism for sharing intelligence information with the private sector.

Figure 3-1 summarizes our findings for each of these three topics. These findings reinforce our belief that effective bi-directional processes will require joint public-private maturation of processes. In short, linking the right people with the right information at the right time requires improving existing implementation approaches, including organizational structures, processes, and staff resources to realize systemic improvement.

Figure 3-1. Summary of Findings

NIAC Task: Assess the Overall Progress and Status of Intelligence Information Sharing

The NIAC found:

- Infrastructure protection is not receiving the high priority that is commensurate with its vital importance to the Nation's economic health and security. The Federal Government must recognize this priority through policy emphasis that drives action.
- The private sector has broad capabilities that can be better leveraged by the government. Private sector integration into the intelligence cycle can contribute insight and analysis, *in addition* to new data.
- Public and private incentives for information sharing are not aligned to serve the infrastructure protection mission. This can result in conflicting value propositions that affect fundamental discussions about how and what information is shared.
- The complexity of the Federal intelligence-sharing enterprise is often confusing to the private sector, resulting in missed opportunities for collaboration that would benefit the Nation.
- DHS has the mission and authority to serve as a champion and leader for infrastructure protection within the Federal Intelligence Community, and has developed critical linkages with private sector owners and operators that can be leveraged as an important information source for Federal intelligence.

NIAC Task: Assess the Role of Fusion Centers as a Mechanism for Sharing Intelligence Information with the Private Sector

The NIAC found:

- Fusion centers are an effective way to leverage government resources across Federal, State, and local partners. Centers that have a mission of critical infrastructure protection can be effective mechanisms for private sector information sharing and critical asset protection. However, not all fusion centers have this capability.
- An ideal mechanism would have two key characteristics: a *primary* mission of infrastructure protection and resilience, and an operating structure that *facilitated* private sector participation.
- The majority of fusion centers, however, have a primary law enforcement mission, which makes private sector participation modest at best.

NIAC Task: Assess Ways to Improve Counterintelligence

The NIAC found:

- “Counterintelligence" has specialized meaning in the Intelligence Community that is largely outside of the realm of the private sector. The term "counterterrorism information" more accurately describes the information the private sector is attuned to and to which it can contribute.
- The private sector has knowledge and capability to *help solve problems*. Providing data is only one capability; the sectors can contribute to analysis that drives data needs.
- The sectors can provide unique information not realized from other sources.
- Counterterrorism is an excellent example of an area where the government could more effectively leverage private sector capabilities.

Table 3-1 summarizes our specific findings, presented in seven topic areas. There are five topics that address the main tasking on the overall progress of intelligence information:

- Authority and policy
- Implementation of authority
- Leveraging the capability of the private sector to reduce risk
- Information content
- Information delivery

The final two topics address the other two taskings:

- Counterintelligence/Counterterrorism
- Fusion Centers

Table 3-1. Specific Findings

Findings	
1. **Authority and Policy:** Is the appropriate authority and policy structure in place, and is it clear and understood by all partners?	A. Federal law and policy clearly include the private sector as a customer of the Federal Intelligence Community. B. DHS has clear authority to share with the private sector the counterterrorism and critical infrastructure protection information developed by the Federal Intelligence Community. C. The priority of critical infrastructure protection, both within parts of DHS and the Federal Government at large, appears to be low and is not commensurate with the important role of critical infrastructure in the Nation’s security and economy. D. There is currently not an effective process to engage—in a systematic and *sustained* manner—senior executives in the private sector with their counterparts in government.

Findings	
2. Implementation of Authority: Do the organizational structures and processes enable effective integration of threat, vulnerability, and consequence information within and across public and private sector partners?	A. DHS's implementation of its authority within the Federal Intelligence Community for information sharing with private sector owners and operators is uneven, reflecting an early stage of maturity in an evolving model for information sharing. For the Federal Intelligence Community at large, information sharing with owners and operators appears to be similarly constrained, in this case by unfamiliarity with the private sector as a customer. Even where understanding is good, processes remain deficient. B. The Federal Intelligence Community often does not understand what information the private sector needs, nor does the private sector always understand the actual capabilities and missions of the Intelligence Community. C. The separation of the original DHS Directorate for Information Analysis and Infrastructure Protection into two separate organizations appears to have adversely affected the sharing and fusing of intelligence information in overall public-private risk-management processes. D. The complexity of roles and responsibilities in Federal intelligence-sharing enterprise is confusing to the private sector, and it lacks the clarity needed to be truly effective.
3. Leveraging the Capability of the Private Sector to Reduce Risk: Do the Federal Intelligence Community and the private sector understand and leverage each other's capabilities?	A. The unique knowledge and analysis capabilities offered by the private sector are not widely understood by government, and where they are understood, the processes to leverage this capability are not in place. B. Differing incentives and disincentives, within and across the Federal Intelligence Community and the private sector, make a shared value proposition that encourages information sharing difficult to define and achieve. C. Intelligence information-sharing mechanisms between the private sector and the Federal Government are complicated, at times confusing to the private sector, and may be redundant and/or conflicting. As a result, engagement through trusted personal relationships remains a primary means of facilitating the flow of needed intelligence information. D. The private sector is willing and able to share information with government that may be useful in counterterrorism efforts. However, the private sector perceives that the government is not yet prepared to receive information from the private sector, to act on it, or to provide feedback on whether the information was investigated and found to be useful. E. There are emerging models of successful bi-directional intelligence information sharing, including the engagement process used by some Sector-Specific Agencies (SSAs) and three DHS pilot efforts: 1) the Classified CIKR Engagement Working Group, 2) HITRAC Classified Information "Reading Room," and 3) an effort with the Banking and Finance Sector to define intelligence-sharing protocols. F. There are also models of success for Sector Coordinating Councils

Findings	
	(SCCs); these should provide lessons successful engagement with owners and operators, starting with the fundamental need to define and inform the companion SSA on sector intelligence needs.
4. **Information Content:** Is there a bi-directional flow of products, with Federal products that meet sector requirements, and private-sector products that meet Federal requirements?	A. The private sector generally does not receive the intelligence information it needs, though this varies somewhat across sectors. With the exception of asset-specific threats, the majority of information received is reactive to events rather than usefully predictive. B. In addition to finished intelligence products, fragmentary information is highly valuable to the private sector, particularly given the need for timely information. Information otherwise viewed as fragmentary or not relevant by the Federal Intelligence Community may in fact be highly relevant within the context of sector operations. C. Nearly 10 years after 9/11, the DHS Office of Intelligence and Analysis is now developing a pilot program, the Sector Information Needs process, to engage the private sector in defining owner/operator requirements. D. DHS is in the nascent stages of using predictive analytics. In comparison, other components of the Federal Intelligence Community and the private sector already make effective use of these tools. DHS should leverage this powerful, state-of-the-art approach to provide timely threat analysis and warning.
5. **Information Delivery:** Are there effective bi-directional processes that enable the timely sharing of information between the Federal Intelligence Community and the private sector?	A. Intelligence sharing processes, tools, and products are improving but need to be significantly better. This includes, for example, improved classified and unclassified briefings and *timely* delivery of information useful for prevention and risk mitigation. B. Currently, the use—and usefulness—of the Homeland Security Information Network – Critical Sectors (HSIN-CS) as a preferred mechanism for sharing is modest at best. On the whole, HSIN-CS does not meet the requirements of private sector owners and operators, and its technology platform does not take advantage of current, off-the-shelf tools that can significantly contribute to meeting the time-critical needs of threat analysis. However, the recent DHS business-case assessment for HSIN acknowledges these deficiencies and is driving plans to remediate them. C. The private sector reaches out to multiple sources to meet its intelligence needs, including trusted personal relationships, trade associations, various DHS components, other government agencies such as the FBI, Sector-Specific Agencies, sector Information Sharing and Analysis Centers, fusion centers, and State and local law enforcement. While it is important to note that the "value proposition" of various sources and mechanisms varies across sectors, there is a common concern over receiving redundant, late, or conflicting information. D. The Critical Infrastructure Partnership Advisory Council (CIPAC)

Findings	
	structure—and its constituent members, which include owners and operators that are members of their respective Sector Coordinating Council and their representative trade or equivalent organizations—is an essential foundation for effective information sharing. As part of this foundation, trade associations play an essential role in information sharing. For example, they may be the only formal information sharing mechanism for small and medium-sized businesses.
6. **Counterintelligence/ counterterrorism:** What information and capability can the private sector contribute to problem solutions in protecting the Nation's infrastructure?	A. "Counterintelligence" has specialized meaning in the Intelligence Community that is largely outside of the realm of the private sector. The term "counterterrorism information" more accurately describes the information the private sector is attuned to and to which it can contribute. B. The private sector has knowledge and capabilities that can help anticipate and solve problems. Providing data is only one capability; the sectors can provide context and contribute to analysis that drives data needs.
7. **Fusion Centers:** What is the effectiveness of the fusion center model in meeting the needs of private-sector critical infrastructure owners and operators?	A. The fusion center model appears to be effective for law enforcement and first-responder engagement with State, regional, and local communities. The use of fusion centers for sharing intelligence information with the private sector varies dramatically across locations and sectors, but overall seems comparatively modest. There are, however, several good models of success in this regard.

These findings are amplified below, drawing material from the five sector case studies (Appendices B through F), additional interviews and briefings, open source research, and contextual discussions among the Study Group and Working Group. The following appendices provide background material that frames much of the content of these findings.

- Appendix I. The Federal Structure for Intelligence Information Sharing
- Appendix J. The DHS Structure for Infrastructure Protection
- Appendix K. Federal Programs and Processes
- Appendix L. Homeland Security Information Network – Critical Sectors
- Appendix M. Fusion Centers and their Role in Intelligence Sharing with the Private Sector
- Appendix N. Examples of Effective Practices Cited in Case Studies
- Appendix O. Sources

3.2.1 Authority and Policy

A. Federal law and policy clearly include the private sector as a customer of the Federal Intelligence Community.

Federal laws and policies establish the private sector as a customer of the Federal Intelligence Community. The most important of these laws, policies, and implementing strategies are:

- Homeland Security Act of 2002
- Intelligence Reform and Terrorism Prevention Act of 2004
- Implementing Recommendations of the 9/11 Commission Act of 2007
- Homeland Security Presidential Directive 7 of 2003
- Executive Order 13311 (2003)
- Executive Order 13388 (2005)
- National Infrastructure Protection Plan (2002, 2009)
- Information Sharing Environment Implementation Plan (2006)
- National Strategy for Information Sharing (2007)

Appendix G (DHS Authorities in Intelligence Information Sharing) addresses the legal authority for DHS to establish inter-agency procedures for sharing intelligence and homeland security information with the private sector. It summarizes the major authorities for public-private intelligence and information sharing.

B. DHS has clear authority to share with the private sector the counterterrorism and critical infrastructure protection information developed by the Federal Intelligence Community.

The information coordination authorities of DHS are listed in Section 201 of the Homeland Security Act as responsibilities given by Congress to the Under Secretary for Information Analysis and Infrastructure Protection. These authorities include, but are not limited to, the following:

> (1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information in order to—
>
> > (A) identify and assess the nature and scope of terrorist threats to the homeland;
> >
> > (B) detect and identify threats of terrorism against the United States; and
> >
> > (C) understand such threats in light of actual and potential vulnerabilities of the homeland.
>
> (2) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).
>
> (3) To integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities.
>
> (4) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining such information from other agencies of the Federal Government.
>
> (5) To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution

> systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems.
>
> (6) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

That DHS has the authority to coordinate intelligence information on critical infrastructure between the Federal Government and the private sector was recognized by all of those interviewed and by each of the case studies. The Commercial Facilities Sector, in particular, made this point as its first case study finding: "DHS has been given primary responsibility within the Federal Government to share intelligence-derived counterterrorism and critical infrastructure protection (CIP) information with the private sector, including the Commercial Facilities Sector, and it has all of the necessary legal authorities to do so. DHS' implementation of programs and mechanisms to undertake this mission, however, has been slow to mature."

C. The priority of critical infrastructure protection, both within parts of DHS and the Federal Government at large, appears to be low and is not commensurate with the important role of critical infrastructure in the Nation's security and economy.

Many of the shortcomings of information sharing can be traced to this fundamental problem, which was cited repeatedly in discussions with senior executives. Simply put, when critical infrastructure protection and resilience is a low priority, public-private information sharing suffers.

The issue appears to have several root causes:

- The reduced sense of urgency to secure the nation's critical infrastructure as time elapsed since the events of September 11, 2001
- The day-to-day operational demands from multiple domestic and international crises (including wars in Iraq and Afghanistan) faced by DHS and other Federal agencies since 2001
- Challenges in coordinating the 22 agencies folded into the new Department of Homeland Security.

The National Security Preparedness Group in its 10th anniversary report card on implementing the 9/11 commission recommendations found that, while significant progress has been made since 9/11, major challenges remain to protect the nation from a catastrophic terrorist event. Chief among these are bureaucratic inertia in adjusting to emerging threats, lack of unity and progress among the multiple agencies that have domestic counterterrorism responsibilities, confusion over command responsibilities during catastrophic disasters, unwieldy congressional oversight of the homeland security mission, and ambiguities over the budget and personnel authorities of the Director of National Intelligence.[11]

While the Council recognizes that DHS faces challenges in its several mission areas, the overall priority of critical infrastructure appears to be low in implementation and practice compared to other mission areas.

[11] See, National Security Preparedness Group, *Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations*, Bipartisan Policy Center, September 2011, http://www.bipartisanpolicy.org/sites/default/files/CommissionRecommendations.pdf.

D. There is currently not an effective process to engage—in a systematic and *sustained* manner—senior executives in the private sector with their counterparts in government.

We find the CIPAC structure for public-private information to be a highly effective approach in general. However, the level of executive engagement varies considerably, both across different Sector Coordinator Councils, and within individual councils. There is, for example, generally good representation of Chief Security Officers or their equivalents. And while we find that while there has been success through the CIPAC mechanism on strategic issues, there has not been a comparable emphasis on executive-level engagement for operational issues. In the face of a massive disruption or disaster, however, there is presently no assurance that senior executives – who can make decisions about the commitment of private resources – will be able to effectively coordinate with government in *responding jointly to National challenges*. Established, tested and accepted protocols are needed to ensure decision makers are connected and ready to act. A disaster is no time to exchange business cards.

3.2.2 Implementation of Authority

A. DHS's implementation of its authority within the Federal Intelligence Community for information sharing with private sector owners and operators is uneven, reflecting an early stage of maturity in an evolving model for information sharing. For the Federal Intelligence Community at large, information sharing with owners and operators appears to be similarly constrained, in this case by unfamiliarity with the private sector as a customer. Even where understanding is good, processes remain deficient.

DHS has broad authority to coordinate the sharing of intelligence information between government and the private sector owners and operators of the nation's critical infrastructure. Yet, in many conversations with public and private sector experts, we heard that DHS was not fully implementing its authorities. For example, the Commercial Facilities Case Study team noting in its finding 3: "DHS is responsible for sharing with the private sector intelligence-derived information collected by other Federal agencies, but it can only do so if the originating agency concurs. Because DHS's intelligence analysis capabilities are still maturing, it is viewed as a junior partner within the IC and, as a result, is disadvantaged as an advocate for sharing information with the private sector. In addition, the information that the originating intelligence agencies provide to DHS has often already been analyzed and filtered, which provides DHS analysts little or no context and which excludes potentially valuable but fragmentary CIP information from being shared with private sector owner/operators who may recognize the value of the information when the Government does not."

Perhaps the most compelling reason DHS has not fully implementing its authority is because it is a new Federal department in a fairly early stage of organizational maturity for many of its programs, including information sharing. As noted in the Banking and Finance case study, one way to understand the role of maturity in the development of organizations is the Capability Maturity Model (CMM) developed by Carnegie Mellon University. Although no direct application of the model to intelligence-sharing partnerships could be found, the stages of the model might be loosely applied to such partnerships.[12] The five stages of CMM and definitions possibly applicable to intelligence-information sharing organizations are:

> **Stage 1: Initial** – first attempts at sharing of information between public and private sectors is usually based on personal trust relationships and past experience in dealing with each other in crises or other significant events.

[12] See Mark C. Paulk, Charles V. Weber, and Mary B. Chrissis, "The Capability Maturity Model: A Summary," *Institute for Software Research*, Paper 2 (1999), http://repository.cmu.edu/cgi/viewcontent.cgi?article=1013&context=isr&sei-redir=1#search=%22Capability%20Maturity%20Model%3A%20Summary%22

Stage 2: Repeatable – building upon a few examples that work to make the exchange more frequent and across a broader range of issues.

Stage 3: Defined – organizing the processes in a more defined manner with roles and responsibilities communicated and expectations categorized.

Stage 4: Managed – managing the process with a goal to improve product and process quality.

Stage 5: Optimizing – continuous improvement through a feedback system and process change management.

To more understand why DHS may not be fully implementing its authorities, the Council conducted a separate examination of the intelligence component. We uncovered three general findings:

- **The Cold War information sharing model ("need-to-know") still pervades many government agencies.** This model and its accompanying mindset do not appear to be consistent with the asymmetrical threats facing the Nation today. The model may be seriously impeding the sharing of intelligence information with the private sector.
- **The 9/11 Commission recognized the need for the government to share critical infrastructure protection information with the private sector.** Revised Executive Order 12333 explicitly states that the private sector is a legitimate consumer of intelligence, but intelligence agencies have not established a process for communicating critical information to the appropriate sectors.
- **The vast majority of intelligence information sharing from the U.S. government to the private sector is done on the basis of personal relationships.** There is no programmatic effort on the part of the Federal Government to communicate such information to the private sector except by publishing it on unclassified bulletin boards, many of which are duplicative.

Findings related to the individual components of the intelligence cycle – requirements, collection, analysis, and dissemination – are summarized in Figure 3-2.

Figure 3-2. The Components of the Intelligence Cycle

The intelligence component findings as to why DHS may not be fully implementing its authorities to share intelligence information with the private sector include:

Requirements

- Most members of the Intelligence Community are not knowledgeable of critical infrastructure intelligence requirements. There currently is not a formal process in place to identify critical infrastructure sector intelligence requirements and to disseminate these to the Community for collection, analysis, and distribution.
- Steps are being taken to remedy this problem on a sector-by-sector basis, but a more formal process would likely be more effective and could be implemented more consistently throughout the Intelligence Community and across all sectors. Included in the formal requirements process should be an efficient means of deconflicting priorities between, for example, critical infrastructure and law enforcement when the withholding of information causes continuing harm to certain sectors.

Collection

- Private sector infrastructure protection intelligence collection requirements are not considered in the annual Intelligence Community collection tasking process. Without specific requirements to collect information of value to the private sector, it is unlikely that intelligence collectors will compile information to enable the private sector to manage risks and mitigate threats.
- The Intelligence Community is structured to generate and disseminate "finished intelligence." Many leads and bits of fragmentary information are discarded if they do not fit in with a finished intelligence product. Those fragmentary bits of information may be very significant to the owners and operators of critical infrastructure and are lost because the intelligence dissemination system either does not recognize the potential value to the private sector or has no incentive to share it with the private sector.

Analysis

- The vast majority of intelligence information provided by Federal Government agencies, including DHS, FBI and others, to the private sector is reactionary. Typically, the private sector receives no more information from government entities than they would garner from news media reports. There is very little "anticipatory", or pro-active, information flow from the public to the private sector. The DHS-provided proactive disseminations are currently at such a high level that private sector recipients cannot take useful action. Private sector organizations, such as Michael Stapleton Associates in New York, have filled this void by providing actionable analyses of current threats. The government's infrastructure protection efforts are seriously undermined by its failure to provide meaningful guidance, actionable advice, and forward-looking assessments.
- DHS does not have a sufficient number of analysts trained in both intelligence and critical infrastructure. DHS does not have enough seasoned intelligence analysts or senior managers to have credibility with the rest of the Intelligence Community. Even in the I&A Directorate, there is no standardized training and/or selection process for the Intelligence Officers currently being fielded in the fusion centers. Most do not come from a background in the IC. Likewise, DHS does not have the private sector expertise to be able to understand the infrastructure protection information requirements of the private sector.

Dissemination

- There is no consensus within the Federal Homeland Security and Intelligence Communities as to what constitutes critical infrastructure protection information that should be shared with the private sector. There is no established information sharing processes with the IC and the private sector. As it stands, the intelligence information obtained by the private sector is usually generated through personal relationships. In most cases, individuals with experience in both the public and private sectors are most effective at information sharing.
- DHS is charged with disseminating critical infrastructure protection information derived from intelligence reporting but is not the originating agency. Since it does not "own" the information, it is powerless to disseminate information unless the originating agency agrees. DHS has the responsibility but no authority. "Ownership" of the information and the need to build consensus in drafting disseminated documents for the private sector are both obstacles to disseminating IC information to the private sector.
- Because DHS is not an intelligence collection agency, it is often unsure of what information can be shared with the private sector. This often results in excessive caution (i.e., incentives to share less rather than to share more) to

ensure that it does not inadvertently reveal sources and methods or compromise ongoing investigative efforts. The relative lack of experienced IC analysts and senior IC managers in DHS is partly to blame for this.

- Because of the lack of actionable information from DHS, the private sector is tending toward developing its own resources and increasingly to bypass DHS as its primary or main source of intelligence. The classification system was not found to be a central issue, although improvement in the granting of security clearances was important to some sectors. Of more importance was the paradigm, or culture, within which CIP intelligence information was not accorded sufficient priority.

These findings are consistent with the overall observation that the intelligence information sharing partnership under DHS is still in a relatively early stage of maturity. Many of the findings and conclusions of the intelligence component were echoed in the September 2011 report of the Intelligence and National Security Alliance, "Intelligence to Protect the Homeland."[13]

The Partnership for Public Service used a different methodology to examine the maturity of DHS as a whole and came to a similar conclusion.[14] Their study noted that the creation of DHS was the right decision and worth the effort, but that the merger of 22 separate organizations "initially resulted in mission overlaps and policy shortfalls, confused functional and operational roles and responsibilities, dissatisfied citizens and employees, intense political pressures and public scrutiny." The reported stated: "Our interviews and research presented a picture of DHS leaders operating with the best of intentions in a crisis atmosphere, and with an unprecedented sense of urgency and determination to avoid another terrorist attack. But they were hampered by inadequate time to plan, to put the complex new department together and to build internal cohesion. They faced disorganization, resistance from merged entities, turf wars, low employee morale and a wide range of management shortcomings involving procurement, financial controls, information technology and the handling of contractors—issues that remain today."

B. The Federal Intelligence Community often does not understand what information the private sector needs, nor does the private sector always understand the actual capabilities and missions of the Intelligence Community.

Private sector executives frequently noted that a mutual lack of understanding between the private sector and the Intelligence Community about their respective needs and operating models was a source of many problems. This view was supported in several of the case study findings. Our interviews revealed a multifaceted problem.

- The Intelligence Community has very few analysts trained in areas of critical infrastructure, nor is there currently in place a training program to address this lack of understanding. Most intelligence analysts, who develop some expertise in this area, do so through "on-the-job" training.
- Although some private sector chief security officers (CSO) come from an intelligence background, most do not. These latter CSOs often do not understand the Intelligence

[13] Intelligence and National Security Alliance and Homeland Security Intelligence Council, "Intelligence to Protect the Homeland: taking stock ten years later and looking ahead," http://images.magnetmail.net/images/clients/INSA/attach/INSA_Homeland_Security_Intelligence.pdf. The White Paper's key recommendations can be found on pp. 16-17.

[14] Partnership for Public Service and Booz/Allen/Hamilton, *Securing the Future: Management Lessons of 9/11*, August 2011, available through http://www.ourpublicservice.org/OPS/publications/viewcontentdetails.php?id=164. The quotations are from pages 1-2.

Community's capabilities for providing intelligence to the private sector, nor the procedures necessary to follow to receive intelligence-derived products.

- As reflected in the findings of the intelligence component of the study, the intelligence requirements of critical infrastructure currently are not part of the collecting or reporting process of the Intelligence Community. Analysts are not normally tasked to work on issues related to critical infrastructure and do not have many procedures in place to produce intelligence products of use to the private sector.
- Embedded intelligence analysts in the sectors, and embedded sector representatives in the Intelligence Community would greatly improve mutual understanding and appreciation of each other's responsibilities and capabilities, but such programs are relatively few in number across government and the 18 sectors.
- There is misperception on the part of intelligence analysts that the private sector has little to contribute to understanding threats to national security, and on the private sector side that the Intelligence Community knows far more than it is sharing.

In a pilot effort to improve understanding of critical infrastructure needs, the Oil and Natural Gas Sector Coordinating Council and I&A initiated a Sector Intelligence Needs (SINs) process designed to define what the intelligence requirements of the ONG sector were and to identify I&A capabilities to meet those requirements. The Chemical and Commercial Facilities Sectors have had initial contact with I&A about the SINS process and – as discussed later in this section – the Banking and Finance Sector has initiated its own process of communicating its intelligence needs to DHS and other Federal partners.

C. The separation of the original DHS Directorate for Information Analysis and Infrastructure Protection into two separate organizations appears to have adversely affected the sharing and fusing of intelligence information in overall public-private risk-management processes.

The difficulties inherent in the creation of DHS and establishing a coherent organizational structure were reflected in the initial joining, and then separation, of the functions of intelligence analysis and infrastructure expertise – both of which are vital elements for an effective sharing of intelligence information between government and the private sector owners and operators of critical infrastructure. The reorganization of IAIP appears to have weakened the intelligence information sharing process for the nation's critical infrastructure. In 2005 the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) was established as a hybrid organization intended to bridge the gap between I&A and IP. Discussions with current and former DHS officials involved with HITRAC indicated that the blending of intelligence analyst with sector specialists never really worked as planned. The separation of IAIP into the Office of Intelligence and Analysis (I&A) and the Office of Infrastructure Protection (IP) is discussed in Appendix J, The DHS Structure for Infrastructure Protection.

HITRAC appears to have increased the range and sophistication of its services and products since its inception. Yet the focus on, and delivery of products for, the critical infrastructure mission appears to have diminished. HITRAC has expanded its scope to include other DHS elements, including, for example, direct support to DHS leadership in emergency response situations. This additional scope has reduced the availability of support for infrastructure. This reduced focus on the infrastructure mission is reflected in the reduction of HITRAC analysts dedicated to the infrastructure mission. When HITRAC was initially stood up, there were 30 analyst positions. Today there are six.

We find the HITRAC *model* to be an effective approach to synthesizing the elements of risk management, one that is particularly crucial given the split of risk-management elements between I&A

and IP. However, without appropriate priority for the infrastructure mission, HITRAC will fall short of its potential as a contributor to improved public-private risk management.

There are however, significant initiatives underway that may address this issue at the top levels of the Department. Among the most important of these is the DHS Private Sector Information Sharing Working Plan, tasked by the Secretary of Homeland Security and led by the I&A Under Secretary.[15] The purpose of the plan is to identify and implement practical steps across the Department for improving the DHS partnership with the private sector. One of the four focus areas is to enhance information sharing and accountability to ensure that DHS gets the right information to the right people in a timely manner. Identified objectives include:

- Provide more useful information to the private sector and engage private sector entities in the Standing Information Needs (SINs) process.
- Provide clear guidance to the private sector for handling and dissemination of For Official Use Only (FOUO) information and Controlled Unclassified Information (CUI).
- Increase information to critical infrastructure owners and operators on methods to become more involved in public-private partnerships.
- Increase educational outreach to private sector partners regarding specialized DHS information protection programs to ensure partners that information provided to DHS will be protected from public disclosure or misuse.

For its part, the Office of Infrastructure Protection is reaching out to its various information sharing partners to solicit confidential feedback on its products and services. The purpose, as in the Private Sector Information Sharing Plan mentioned above, is to improve DHS information sharing with its various Federal, State, local, tribal, territorial, and private sector partners.

D. The complexity of roles and responsibilities in Federal intelligence-sharing enterprise is confusing to the private sector, and it lacks the clarity needed to be truly effective.

In general, the multiplicity of entities, the complex "rules of the road" for who to share with, and confusion over their roles is daunting to anyone not intimately familiar with the Federal Intelligence Community. This was a theme heard in many of the case study interviews, although sectors which have a long history of dealing with Federal regulators – such Banking and Finance and Oil and Natural Gas – seem to have more established channels for working with the Federal Intelligence Community. The Chemical Sector in particular noted that, in times of crisis, the multiple reporting requirements and redundant information flows into the sector could be overwhelming to security managers.

This formalized exchange of intelligence information is hampered, however, by the almost universal perception on the part of the private sector that there are too many Federal agencies involved in security issues. A frequent observation heard in the interviews was that companies do not always know to whom to talk for either reporting intelligence-related information or receiving information that may be relevant to their plans or operations. Often, companies reach out to multiple agencies in order not to miss anything; they also feel obliged to file duplicative reports to several agencies requesting the same information. This is not to infer that there should be a single point of information exchange. Indeed, if owners and operators are to be a valued customer for intelligence, agencies should strive to be the best at fulfilling this mission.

[15] The following information about the Working Plan is based on briefings provided to the NIAC by I&A officials in March and August 2011.

A striking example of this confusion is response to the emergence of advanced cyber threats. We found there is no clear understanding of the roles of the various intelligence agencies in reaching out and assisting the private sector. Without a clear mapping of where to engage, the sectors tend to leverage their existing relationships with government to find the cyber support they needed. Often this involved a process whereby industry leaders would appeal directly to DHS (or other SSAs) to create special mechanisms for the sharing of intelligence.

3.2.3 Leveraging the Capability of the Private Sector to Reduce Risk

A. The unique knowledge and analysis capabilities offered by the private sector are not widely understood by government, and where they are understood, the processes to leverage this capability are not in place.

The private sector has progressively developed a wide range of intelligence capabilities spanning the entire intelligence cycle of requirements, collection, analysis, and dissemination. These capabilities may be found in a variety of business structures, including individual companies with internal intelligence units, companies specializing in providing intelligence service and products to others, and associations of security professionals. Some of these capabilities may duplicate similar ones in the Federal Intelligence Community – *often because companies are not receiving the information they need from these sources*. Additionally, however, the private sector has unique capabilities. These include providing privately held information that is not in the public domain and providing context for information that might otherwise be missed or under-valued by the Federal Intelligence Community.

The Council found many examples of this kind of capability being made available through the private sector. One example is in commercially available tools, which can analyze, integrate, and visualize all kinds of data, including structured, unstructured, relational, temporal, and geospatial data. Because of their sector expertise in adapting and using these new technologies, the private sector has capabilities that the Federal Intelligence Community may not be fully aware of. Additionally, the NIAC found examples of where the private sector has provided experts in sector operations to work alongside colleagues in the Department of Homeland Security – at no cost to the government. We believe this is a valuable model of capability leveraging that should be considered for wider use.

B. Differing incentives and disincentives, within and across the Federal Intelligence Community and the private sector, make a shared value proposition that encourages information sharing difficult to define and achieve.

The Federal Intelligence Community emphasizes the “need-to-know.” In contrast, the private sector’s emphasis is more on the “need-to-share.” Safeguarding sensitive information and information sharing are two sides of the same coin: both requirements need to be acknowledged and both need to be effectively implemented if the nation’s interests in critical infrastructure protection and resilience are to be served. Figure 3.3 illustrates several of the major factors in the value propositions of the public and private sectors in regards to the sharing of intelligence information, and how incentives may differ for sharing.

For example, it appears that in the Federal Intelligence Community, possible penalties - to personnel or to an organization – for sharing may outweigh the positive outcomes of sharing. And while with privately-held information the private sector does not have these same classification constraints, we found there are nonetheless constraints on sharing by private sector owners and operators related to competitive concerns and other factors.

Figure 3-3. Some Factors in the Value Propositions for the Sharing of Intelligence Information

Private Sector:

- The private sector operates on core incentives of reputation and profit; intelligence information sharing that protects business continuity supports these incentives.
- The private sector generally will share information with the government in order to fortify the company's - and the industry's - security posture and the attendant business continuity.
- Due to competitive concerns, proprietary and other sensitive information shared with the government must be protected in order to protect company reputation and shareholder value.
- If the private sector does not receive valuable information or feedback from the government, they will be disinclined to continue sharing sensitive information with the government.

Federal Intelligence Community:

- Concern about dissemination of information that could reveal sources and methods of intelligence gathering inhibits timely information delivery to the private sector.
- Incentives to collect private sector critical infrastructure-related information have not been established in the Intelligence Community.
- The intelligence community members —as the collectors and owners of the intelligence information—need specific incentives to share critical infrastructure information with DHS, in order for DHS to then share with the private sector.
- Possible incentives to encourage private sector intelligence collection and dissemination with the IC are:
    - Annual performance review metrics for critical infrastructure intelligence information collected and disseminated.
    - Annual performance review metrics for the timeliness of information shared with the private sector.

C. Intelligence information-sharing mechanisms between the private sector and the Federal Government are complicated, at times confusing to the private sector, and may be redundant and/or conflicting. As a result, engagement through trusted personal relationships remains a primary means of facilitating the flow of needed intelligence information.

All case study sectors reported that personal relationships are critical in acquiring needed intelligence from the government and from peers within industry. Personal dialogue also is invaluable in helping to interpret and validate certain threat information. Personal, trusted relationships will always be important in the sharing of sensitive information. However, to the extent possible, the sharing of intelligence information should be channeled through formal mechanisms.

This multiplicity of sources of intelligence information, and the associated processes for information exchange, greatly complicates the job of industry security officials who must consult with contact after contact, agency after agency, network after network to ensure they have the information they need. In interviews, it was often cited that information is duplicative or can be obtained more readily – and more timely – from CNN. None-the-less, the intelligence *is invaluable* for the specific requirements of a given sector of industry, so the process of consulting source after source is perpetuated.

Case study findings that reflected this overall observation include:

- **ONG Sector** – "The ONG Sector utilizes a wide range of information-sharing tools and mechanisms. HSIN-CS is valued primarily as a reference tool, but it is not deemed too useful for operational, real-time security. Other mechanisms include local fusion centers, the DHS Protective Security Advisors and the ONG Sector Specialist, the Transportation Security Operations Center, local Joint Terrorism Task Forces, FBI, local law enforcement, US-CERT, the ONG SCC, trade associations, contracted private intelligence companies, and others."

- **Commercial Facilities Sector** – “Redundant information sharing programs by various Federal agencies confuse and frustrate private sector users as they attempt to navigate an overly complex information sharing landscape. As a consequence, many have turned to private companies, industry associations and trusted personal contacts, within and outside of Government, to meet their critical infrastructure protection information needs.”
- **Chemical Sector** – “Personal relationships that chemical security managers maintain with Federal Government contacts, law enforcement, and their industry peers are highly important for gathering and interpreting threat and intelligence information.”

D. The private sector is willing and able to share information with government that may be useful in counterterrorism efforts. However, the private sector perceives that the government is not yet prepared to receive information from the private sector, to act on it, or to provide feedback on whether the information was investigated and found to be useful.

In almost all cases, the private sector is willing to share information with government that may be of use to agencies in their various intelligence-related activities, such as counterterrorism, law enforcement, and national security purposes. A frequent complaint heard across the case studies, however, was that government is not providing sufficient feedback to the private sector providers of the information. The private sector does not know if the information it provided was useful or irrelevant, if it was acted upon or ignored. The lack of feedback results in a weakening of willingness to share information in the future.

The Healthcare Sector, for example, noted in one of its findings: “Insufficient mechanisms exist for the private sector to provide intelligence information to the Federal Government. Sector members would also value more feedback on how the government uses the intelligence information it does receive from them. This would build trust by demonstrating that the effort expended in reporting to and communicating with the Federal Government creates benefit, and would motivate further response.”

Owners and operators understand that some information – such as that involving sensitive counterintelligence activities or law enforcement investigations – cannot be reported upon by the respective agencies. Nonetheless, it would greatly benefit the exchange of intelligence information between the public and private sectors if government would institute a policy of routinely responding to or at least acknowledging the receipt of private sector information.

E. There are emerging models of successful bi-directional intelligence information sharing, including the engagement process used by some Sector-Specific Agencies (SSAs) and three DHS pilot efforts: 1) the Classified CIKR Engagement Working Group, 2) HITRAC Classified Information “Reading Room,” and 3) an effort with the Banking and Finance Sector to define intelligence-sharing protocols.

There are in fact clear instances of successful bi-directional sharing. The Chemical Sector has an excellent and productive relationship with the Chemical Sector-Specific Agency and views it as a key, valued information sharing asset for the industry. The strong relationship between chemical security managers and the SSA is valuable in gaining access to and analyzing intelligence from Federal Government sources. The Chemical SSA plays a proactive role in helping chemical companies obtain the intelligence information they need and serving as an advocate of industry concerns and needs within the Federal Government.

The DHS Office of Infrastructure Protection (IP) has initiated two promising pilot efforts designed to encourage bi-directional information sharing and leverage private sector insights. The Classified CIKR Engagement Working Group, convened at the request of the Assistant Secretary for IP, engages cleared representatives of Sector Coordinating Councils who review intelligence data (not finished products) to help the government to determine its relevance, the form it should take to make it most useful, and the manner in which it should be delivered to owners and operators (i.e., who, how, and when). HITRAC has initiated the Classified Information "Reading Room" in which members of critical infrastructure owners and operators who possess clearances can periodically access intelligence data relevant to their sector and review it in a classified facility to determine for themselves what is relevant and useful to take action. A proposal has been made to expand these "reading rooms" to the field tied to the fusion centers this coming year.

In the Banking and Finance Sector, there is currently a very promising endeavor underway between the Financial Services Sector Coordinating Council (FSSCC) and DHS to alert pre-approved executives on emerging threats. The NASDAQ hack, discussed in Appendix B, resulted in FSSCC and senior DHS officials agreeing to develop information-sharing protocols under specific conditions. Accordingly, the FSSCC and DHS are collaborating on developing guidelines for when this information should be shared. FSSCC members believe that a more transparent decision-making process would accelerate the dissemination of information without interfering or undermining criminal and national security investigations.

As noted earlier, the Oil and Natural Sector and DHS Office of Intelligence and Analysis are collaborating on a pilot effort to define Sector Intelligence Needs (SINs) so that the sector may receive the kinds of information it needs. Depending upon the results of the SINs process, it may serve as a model for other sectors wanting to more clearly define their intelligence needs and improve intelligence information sharing with the Federal Government. The sector emphasizes, however, that the agreed upon product must be delivered to all concerned stakeholders and acted upon if it is to be effective.

F. There are also models of success for Sector Coordinating Councils (SCCs); these should provide lessons successful engagement with owners and operators, starting with the fundamental need to define and inform the companion SSA on sector intelligence needs.

In the examples cited in the previous section, for instance, the SCCs also played a central role in communicating sector needs to their respective SSAs through information sharing working groups and other channels. The critical factor is that the SCCs must proactively work with the SSAs to define intelligence requirements, and this process must be preceded by the SCC members coordinating among themselves to clarify what those requirements are. As only the sectors themselves have the sector-specific expertise to identify and validate requirements, the SCC must be proactive and speak with the weight of the sectors behind them. We found that two factors contributing to success in this regard include substantial senior-executive-level participation in SCC activities, and owners and operators who have a strong, active voice in identifying actual *operating issues and concerns*.

3.2.4 Information Content

A. The private sector generally does not receive the intelligence information it needs, though this varies somewhat across sectors. With the exception of asset-specific threats, the majority of information received is reactive to events rather than usefully predictive.

The NIAC found that the intelligence that is delivered to sectors is after the fact – not usefully predictive so that sectors can plan and take action. There appears to be a chain of factors behind this. The NIAC found that, even assuming there is 1) a general willingness to share intelligence information and 2) the existence of information sharing mechanisms to support this, there is still concerns about the Federal Intelligence Community providing the type of information that the private sector needs. This is partly a requirements issue, but also an issue of priority. Even with understanding and priority, though, there are still concerns about lack of training among intelligence analysts as to what to look for in terms of collection and analysis processes that might be of use to the private sector. Classification issues, limited resources, competing priorities, and other factors all influence the quality and timeliness of intelligence information that flows to the owners and operators of critical infrastructure.

With respect to needing proactive information, owners and operators need several key types of information. This includes emerging areas of threats, types of attack modes, and possible mitigation measures. Chief security officers of critical infrastructure are interested in as much operational detail as possible: what kinds of vehicles are used to transport the terrorists; what kind of clothing are they wearing; how did they identify the points of attack on the facility; what kind of surveillance did they employ. Owners and operators want to know, in as close to real time as possible, what threats are emerging, how their assets may be vulnerable, and what mitigation strategies might be employed to prevent intrusions into their systems.

The issue of not receiving adequate intelligence information seemed especially pronounced in the Healthcare Sector, where numerous interviewees indicated that there is no formal set of mechanisms for intelligence information sharing within the sector and that there is need for improvement in the mechanisms for sharing that exist between local facilities and Federal agencies. The Chemical and Commercial Facilities case studies also reported on the need for improved intelligence information content received from government.

DHS provides a vast array of information sources to the private sector. Most of these can be found in the DHS *Private Sector Resources Catalog*, which is organized according to the five mission areas of the Department's Quadrennial Homeland Security Review (QHSR).[16] There is a section under the Preventing Terrorism and Enhancing Security mission area, for example, that lists the tools offered by DHS for "Protecting, Analyzing, & Sharing Information," as well as contacts for further information. While this information may be useful, it is not sufficient to meet the intelligence needs of owners and operators *in a timely and comprehensive manner.*

B. In addition to finished intelligence products, fragmentary information is highly valuable to the private sector, particularly given the need for timely information. Information otherwise viewed as fragmentary or not relevant by the Federal Intelligence Community may in fact be highly relevant within the context of sector operations.

It is important to recognize that the private sector has considerable analytic resources and that these are concentrated in areas of sector specificity. Usually, the private sector specialists are far more knowledgeable of what is or is not important than government intelligence analysts. What may seem important to the government analysts may be mundane or common knowledge to the private sector specialists; what may seem unimportant pieces of data – left on the floor – may be vital information to someone responsible for sector security. The classification of the data is less important than its relevancy to the sector, and that relevancy can best be determined by specialists within the sector itself.

The NIAC believes that law enforcement agencies at all levels of government should consider adding a question to their investigative reports that identify any potential impacts on critical infrastructure that may result from or be part of the incident being investigated. The law enforcement community should

[16] *Private Sector Resources Catalog*, version 3.0, July 2011, DHS Private Sector Office, http://www.dhs.gov/xlibrary/assets/pso-private-sector-resource-catalog-3.pdf. The five DHS mission areas identified in the QHSR are: Preventing Terrorism and Enhancing Security, Securing and Managing Our Borders, Enforcing and Administering Our Immigration Laws, Safeguarding and Security Cyberspace, and Ensuring Resilience to Disasters. See, Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, February 2010, http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

devise a mechanism allowing this impact information to be forwarded to potentially affected infrastructure owners and operators in a timely fashion.

There is a mutual dependency between government and critical infrastructure in that both have pieces of the puzzle. Key information may be gathered by government methods. Absent expertise in sector operations within the Federal Intelligence Community, understanding the relevancy of information resides within the sectors. The challenge is how to get the two sides to talk to one another in a meaningful and productive way. Providing classified briefings to cleared private sector representatives can be useful, but it is not sufficient. Sometimes unclassified information is far more actionable. All of this points to the need for better mechanisms to be established that enable intelligence analysts and sector specialists to interact and share or blend their perspectives and expertise.

That being said, there *is* a recognized need for classified intelligence, and the sectors indicated a strong desire to improve the sharing of this kind of information with the Federal Government. One problem indicated by several of the sectors, but particularly the Healthcare Sector, was that the lack of security clearances hampered their ability to receive and disseminate the information needed to prepare facilities for emergencies. This seems to be a problem especially acute for State-level healthcare employees, who are the ground-level responders to mass casualty events. As noted in the sector's case study report, "The government should place greater trust in the Sector's ability to handle and manage sensitive information, and should make a concerted effort to develop and distribute more unclassified briefings."

C. Nearly 10 years after 9/11, the DHS Office of Intelligence and Analysis is now developing a pilot program, the Sector Information Needs process, to engage the private sector in defining owner/operator requirements.

As earlier discussed, this process has made substantial progress in the Oil and Natural Gas sector, and it is being considered by other sectors. As the process has gone forward, it became clear to all participants that the intelligence needs of the sector can be best defined by sector specialists, and these almost always reside within the private sector. The engagement with the Oil and Gas Sectors started with a presentation to the sector of a draft of what the Office of Intelligence and Analysis thought were sector needs. This is essentially backwards; the I&A should simply first ask the sector what their needs are. There is a collaborative synergy required between the public and private sectors to make the SINs process work effectively, but the process needs to better reflect *sectors as customers*.

D. DHS is in the nascent stages of using predictive analytics. In comparison, other components of the Federal Intelligence Community and the private sector already make effective use of these tools. DHS should leverage this powerful, state-of-the-art approach to provide timely threat analysis and warning.

Predictive analytics is based on a variety of statistical techniques from modeling, data mining, and game theory that enables analysis of current and historical facts to make predictions about future events. In business, predictive models can examine patterns found in historical and transactional data to identify risks and opportunities. Models capture relationships among many factors to allow assessment of risk or potential associated with a particular set of conditions, guiding decision making for candidate transactions. For example, the potential benefits of predictive analytics can play an important role in the financial sector. The Banking and Finance Sector case study found: "The Sector wants to expand the use of predictive analytics and other tools so that the threat information it receives is pre-event rather than post-event. Currently, intelligence-related information received from government is primarily post-event."

An example of predictive analytics is the Signature Analyst for Infrastructure Protection program sponsored by the DHS Science and Technology Directorate (S&T). Geospatial predictive analytics, which examines the geographic relationships between certain events and hundreds or even thousands of factors that influence where events have occurred, can help predict where similar events are likely to take place in the future. This tool has been used in Iraq to predict where Improvised Explosive Devices may be planted and in Los Angeles to predict where certain acts of gang violence might occur.

The broad application of predictive analytic tools seems to hold great promise as a tool to enable sectors to anticipate threats and identify associated mitigation measures to their infrastructure. However, they can be expensive and may be beyond the financial and analytical capabilities of smaller companies.

3.2.5 Information Delivery

A. Intelligence sharing processes, tools, and products are improving but need to be significantly better. This includes, for example, improved classified and unclassified briefings and *timely* delivery of information useful for prevention and risk mitigation.

The Oil and Natural Gas sector, among others, noted that restrictions placed on dissemination of classified briefings and materials severely limited effective preparedness to meet threats that were identified by various government agencies. The ONG sector strongly suggested that such agencies produce and distribute unclassified or FOUO documents at the time of their briefings so this material could be distributed more widely to those in industry who need to implement preventive measures. The fact that many decision makers in the sector, as well as operational personnel, do not hold security clearances make the dissemination of unclassified material even more important.

The Chemical Sector, as well as other sectors, stated that, at times, the information contained in many classified briefings had already been disclosed in media reports. Further, those giving the briefings often did not understand the sector and therefore did not correctly identify the type of information needed by sector security specialists. In this sector and in others, the NIAC found an increased effort underway on the part of both government and their private sector partners to collaborate before meetings to develop more tailored briefings.

In the Healthcare sector interviewees expressed a need for improved mechanisms to get intelligence information from the government to owners and operators. Of particular importance in the Healthcare sector would be information on threat trends and implications for mitigation, so officials would be better informed as to when they should shift their resources from one kind of threat to another.

Of the various information sharing mechanisms hosted by DHS and referenced by those interviewed, HSIN-CS was predominantly identified. HSIN-CS is the primary information-sharing platform between the various critical infrastructure sector stakeholders. The network is intended to enable DHS and critical infrastructure owners and operators to communicate, coordinate, and share sensitive and sector-relevant information to protect their critical assets, systems, functions, and networks. HSIN-CS is provided as a hardware, software, communications and operations platform that can be used at no charge to sector stakeholders. We find, however, that there needs to be improved communication to the sectors of their role in *tailoring this platform to their specific requirements*.

B. Currently, the use—and usefulness—of the Homeland Security Information Network – Critical Sectors (HSIN-CS) as a preferred mechanism for sharing is modest at best. On the whole, HSIN-CS does not meet the requirements of private sector owners and operators, and its technology platform does

not take advantage of current, off-the-shelf tools that can significantly contribute to meeting the time-critical needs of threat analysis. However, the recent DHS business-case assessment for HSIN acknowledges these deficiencies and is driving plans to remediate them.

We found a wide range of views expressed about the utility of HSIN-CS for the sharing of intelligence-derived information, with some sectors considering the network to be very valuable and other sectors hardly ever using the network. All of those interviewed agreed that HSIN-CS was improving and that it had significant potential to be a valuable information sharing tool.

HSIN-CS was a topic addressed in many, but not all, of the interviews held by NIAC to gather information and data for its intelligence information sharing study. Comments on HSIN-CS were heard in subject matter expert (SME) interviews from the Chemical, Commercial Facilities, Healthcare and Public Health, and Oil and Natural Gas case studies. HSIN-CS was not commented on in interviews with SMEs from the Banking and Finance and Intelligence case studies. Altogether, some 80 comments were heard in 35 separate interviews. These interviews revealed a number of core themes surrounding the private sector's criticism of HSIN-CS including:

- Content
    - The information is too broad and sanitized to be of great value to owners and operators concerned with managing risks within their critical infrastructure.
- Timing
    - The information does not arrive in real-time. Except for situational awareness during times of slow moving events (such as hurricanes), the information posted on HSIN often is too late to be useful.
    - It is a "pull" system vs a "push" system, placing the onus on the user to search and retrieve relevant information.
- People
    - With notable exceptions, HSIN-CS often does not reach the right people. The private sector itself could help remedy this issue by more carefully selecting those with a need-to-know within their companies.
- Operations/Administrative
    - The interface is difficult to navigate, resulting in considerable time being spent to locate the needed information.
    - Passwords need to be constantly changed, sometimes resulting in users dropping out of the network entirely because of the extra effort required to maintain privileges.

One of the most important strengths – and weaknesses – of HSIN-CS is that it is meant to be populated by sector-defined membership, information, and delivery mechanisms. Sectors which spend considerable time and resources to develop their HSIN-CS portals – such as Oil and Natural Gas – generally report favorable results with HSIN-CS. Critically, this requires advocacy on the private sector side (usually the SCC) and advocacy on the government side (usually the SSA).

Appendix L reviews the development, status, and plans for HSIN-CS. DHS is currently implementing a HSIN improvement plan which is expected to be fully operational in the October 2012-May 2013 timeframe. The NIAC believes these recent developments are promising, but the "proof is in the pudding." For example, the NIAC strongly agrees that an up-to-date technology platform is needed for HSIN-CS in order to take advantage of commercially available tools and techniques for data and information analysis. The lack of an up-to-date technology platform is a critical failing with respect to threat warnings and response. Taking advantage of commercially-available tools and techniques for data/information analysis could significantly improve the *critical timeliness of threat information*.

C. The private sector reaches out to multiple sources to meet its intelligence needs, including trusted personal relationships, trade associations, various DHS components, other government agencies such as the FBI, Sector-Specific Agencies, sector Information Sharing and Analysis Centers, fusion centers, and State and local law enforcement. While it is important to note that the "value proposition" of various sources and mechanisms varies across sectors, there is a common concern over receiving redundant, late, or conflicting information.

As indicated previously, sector security specialists reach out to multiple sources to acquire, assess, and validate intelligence information that may be of use to their particular industry or asset for which they may be responsible. Each sector – indeed, each sub-sector and individual facilities – tends to develop their own network of sources. The Oil and Natural Gas Case Study outlines the multiple Federal, State and local, private sector, and international sources of intelligence-derived information for the sector. Other sectors have a similarly wide range of intelligence information sources that they use. No single facility in the sector uses all of these sources, but no facility that we were able to discern uses only one source. Several of the most commonly used sources across most of the sectors were as follows:

Trusted relationships – these are reported as being common and highly regarded by all the sectors and all those interviewed. However, as noted by the Banking and Finance Sector, the meaning of "trust" in intelligence information comprises several dimensions:

- The partnership must be established for some time so members can get to know each other
- Each member must see a reason for the information sharing partnership to succeed
- The partnership must have a record of success both in terms of information delivery and honoring any confidentialities that may be requested
- Effective mechanisms must exist for the exchange of information.

Trade associations – The Healthcare, Chemical, Commercial Facilities, and Oil and Natural Gas sectors all indicated that trade associations were an extremely valuable source of information and played a vital role in bi-directional information exchange between the sector and various levels of government. In many cases, trade associations were the single most important source for smaller companies.

NIPP sector partnership model – several of the case studies indicated that the SCC-GCC partnership and the CIPAC umbrella were essential for the exchange of intelligence information between government and the private sector. The Financial Sector – SCC was identified as being especially pro-active and effective.

ISACs – although not active in all the sectors, several sectors (Banking and Finance being a prime example), heavily depend upon the sector ISAC as one of the principal intelligence information nodes. No other organization within the financial sector plays the information sharing role of the FS-ISAC, for instance.

SSAs – the sector-specific agencies are not uniform in their role as an information-sharing nexus for the sector. Some SSAs are highly praised by their private sector stakeholders for doing an excellent job in this respect: the Chemical Sector being an outstanding example. Other SSAs are viewed as playing a key role but one that could be strengthened with additional resources and prioritization.

DHS components – the Department of Homeland Security has the authority to coordinate the exchange of intelligence information between the critical infrastructure and the Federal Government. Many DHS programs have been put into place to implement this authority.[17] Some of these programs are exceptional and some need improvement. The NIAC recognizes this to be an ongoing effort on the part of the Department, and historically in its reports has offered recommendations to help strengthen DHS performance in key mission areas affecting the nation's critical infrastructure.

Other Federal Agencies – in addition to the designated SSAs, several other Federal agencies were noted as being especially active in the sharing of intelligence-related information with the private sector. These included the FBI, which has a long and trusted relationship with private industry; the U.S. Secret Service, which provides both cyber and physical security missions for the Banking and Finance Sector; and – more recently – the National Security Agency which – in conjunction with DHS and the Department of Defense – is working more closely with the private sector to counter cyber threats.[18]

One basic model for bi-directional exchange of intelligence requirements and products – which appears to be similar to practices successfully used by several sectors – would have the following sequence of core participants and characteristics.

- An information sharing working group, which operates under the auspices of the Sector Coordinating Council. This group is charged with identifying information requirements of the sector and vetting them through SCC participants.
- The SCC, serving as the voice for the sector to deliver these requirements through the Sector Specific Agency. The SCC must be proactive in asserting its role of representing sector needs.
- The SSA, which must have the extensive sector knowledge necessary to understand and champion these needs.
- DHS, which must deliver these needs to the Federal Intelligence Community and serve as a champion, both for owner and operator needs and for articulating the private sector capabilities that can leverage Federal capabilities.
- The Federal Intelligence Community, which must incorporate owner and operator needs into specific taskings.

D. The Critical Infrastructure Partnership Advisory Council (CIPAC) structure—and its constituent members, which include owners and operators that are members of their respective Sector Coordinating Council and their representative trade or equivalent organizations—is an essential foundation for effective information sharing. As part of this foundation, trade associations play an essential role in information sharing. For example, they may be the only formal information sharing mechanism for small and medium-sized businesses.

Trade associations comprise an important element of CIPAC. In some cases, such as the Real Estate Roundtable (http://www.rer.org/) in the Commercial Facilities Sector, associations were instrumental in the creation and success of the SCC itself. Their leadership, coordination, and information sharing roles in the sectors are essential to the public-private partnership model established by the NIPP and operationalized through CIPAC. Each of the sector case studies underscored the critical role that trade and industry associations play in information sharing within their sectors. Most associations have well-

[17] See the DHS *Private Sector Resources Catalog*, version 3.0, July 2011, referenced earlier in this section.

[18] See, for example, "US Security Agency Opens to Outsiders on Cyber Safety," Reuters, September 20, 2011, http://www.reuters.com/article/2011/09/20/usa-cyber-nsa-idUSS1E78J19N20110920.

established structures and information sharing mechanisms that allow them to push out time-critical and general threat information affecting their member companies. Our interviews with companies of all sizes and in all sectors revealed that the association committees, publications, and, information systems comprise one of the essential conduits for informing them about risks to their infrastructures and facilities. This is particularly true for smaller companies for which communication from their trade association is often the only information they receive about sector risks and preparedness. In addition, companies in specialized subsectors noted that their trade association often provides more tailored information that matched their needs. Figure 3-4 presents findings from the Chemical and Commercial Facilities Sectors.

Figure 3-4. The Importance of Industry and Trade Associations as Information Conduits

Two sectors highlight the importance of industry and trade associations in information sharing:

- **Chemical Sector –** Collaboration on security is typically organized through chemical industry associations, such as the American Chemistry Council (ACC), the Society of Chemical Manufacturers and Affiliates (SOCMA), the Institute of Makers of Explosives (IME), the National Association of Chemical Distributors (NACD), and the International Liquid Terminals Association (ILTA). Accordingly, each is represented on the Chemical Sector Coordinating Council. Small companies we interviewed told us that security responsibilities often represents a portion of a security manager's role, allowing only enough time to work through their association rather than access online government resources. As a result, the chemical sector case study concluded that the continued participation of industry associations in Chemical Sector CIPAC discussions is essential to successful information sharing within the sector.
- **Commercial Facilities Sector –** The enormous size and diversity of commercial facilities dictates the need for multiple, smaller industry associations to facilitate information sharing. Owners and operators, driven by common information needs, have formed groups focused primarily on security and information sharing, either in sector-supported organizations or sub-groups of established industry associations. These include the Real Estate Roundtable, the Real Estate Information Sharing and Analysis Center (RE ISAC), the Building Owners and Management Association (BOMA), the Retail Industry Leaders Association (RILA), the American Hotel and Lodging Association (AH&LA), and National Retail Federation (NRF). These groups have enormous reach. For example, BOMA can push out information to its 16,500 members and 91 local BOMA chapters, and the RE ISAC can send information out to 150,000 names on its mailing list. Some small and more specialized industry associations play an equally important role for their members. As a result, twelve of the thirty representatives on the Commercial Facilities Sector Coordinating Council are from industry associations.

3.2.6 Counterintelligence/Counterterrorism

A. "Counterintelligence" has specialized meaning in the Intelligence Community that is largely outside of the realm of the private sector. The term "counterterrorism information" more accurately describes the information the private sector is attuned to and to which it can contribute.

Overall, the sharing of counterintelligence across the infrastructure sectors is very limited as there is uncertainty in the private sector as to what counterintelligence actually means. In the sectors we reviewed, "counterintelligence" is usually equated with "counterterrorism." More narrowly, multinational companies often do cooperate with the U.S. Government in counterintelligence within the context of their overseas operations. For example, multinational corporations in the Oil and Natural Gas sector have extensive contacts with intelligence agencies from both the United States and host countries, and some of this exchange of information involves counterintelligence issues.

As shown in Figure 3-5, the Office of the Director of National Intelligence has identified potential areas for cooperation. The NIAC does not believe, however, that the National Counterintelligence Executive has sufficiently explained to the private sector how cooperation might be accomplished. One component of the counterintelligence initiative that seems to be lacking is education so owners and operators understand what is being asked of them and have confidence that the information they provide will be protected from disclosure.

Figure 3-5. Possible Owner and Operator Contributing to Counterintelligence

The 2009 *National Counterintelligence Strategy of the United States*, points to five areas of possible owner and operator contribution to the national counterintelligence mission: [19]

- *Integrating counterintelligence with all aspects of cyber*, including computer network operations, workforce development, education, and awareness programs.
- *Assuring the supply chain* as U.S. companies increasingly globalize their business structures and practices, which present foreign intelligence services with new avenues for penetration and exploitation of the U.S. government through its acquisition processes.
- *Protecting the U.S. global economic advantage*, its trade secrets, and technological know-how, by identifying and protecting the nation's critical assets and infrastructure.
- *Advancing Intelligence Community capabilities* through research and development in order to anticipate and identify emerging technical threats.
- *Reaching outward to private sector partners for information* critical to targeting foreign intelligence activities and defending national security.

The NIAC finds that the owners and operators are interested and willing to contribute counterterrorism information, but require better guidance on what is useful and how this information can be applied for mutual benefit.

B. The private sector has knowledge and capabilities that can help anticipate and solve problems. Providing data is only one capability; the sectors can provide context and contribute to analysis that drives data needs.

The private sector has progressively developed a wide range of intelligence capabilities spanning the entire intelligence cycle of requirements, collection, analysis, and dissemination. The ability to provide counterterrorism *information* can be augmented by the capability 1) to define what information is important through contextual knowledge and 2) to provide analytic resources (analysts, tools and processes) to provide timely assessment of this information. The previously described Classified CIKR Engagement Working Group within the DHS Office of Infrastructure Protection is designed to do just that.

3.2.7 Fusion Centers

A. The fusion center model appears to be effective for law enforcement and first-responder engagement with State, regional, and local communities. The use of fusion centers for sharing intelligence information with the private sector varies dramatically across locations and sectors, but overall seems comparatively modest. There are, however, several good models of success in this regard.

The use of fusion centers as an information-sharing mechanism varies considerably across the sectors, but generally seems underdeveloped. The Healthcare sector, for example, reports that fusion centers

[19] See http://www.ncix.gov/publications/policy/NatlCIStrategy2009.pdf.

are “poorly connected to sector members in general and hospitals in particular.” Commercial Facilities reports that “fusion centers do not consistently have counterterrorism or critical infrastructure protection missions, or engage the private sector in information analysis and dissemination.” The Chemical Sector found that “fusion centers do not appear to play a big role in information sharing within the Chemical Sector…with some centers reaching out to the local chemical companies and providing useful information and others not engaging with chemical companies at all.” The Oil and Natural case study found: “The use of fusion centers as an information-sharing mechanism varies considerably across the ONG Sector, with most interaction with fusion centers occurring with local ONG facilities rather than with their corporate headquarters. One outstanding ONG-fusion center partnership was cited: the West Virginia Intelligence Fusion Center. This partnership was held as a model for other centers looking to improve outreach efforts to the private sector.”

Within DHS, the Office of Intelligence and Analysis State and Local Program Office coordinates the Department and other Federal agency support to 72 State and major urban area fusion centers nationwide.[20] I&A currently has nine regional directors and 69 intelligence officers deployed to 69 fusion centers. While DHS provides guidance and analyst support, each center was established by a State, local, or regional jurisdiction to address specific issues of local concern which may not include critical infrastructure protection. Although DHS and the FBI are attempting to establish baseline capabilities across all fusion centers, the Federal Government has little control over whether the limited funding it provides to State and local jurisdictions are actually being apportioned to fusion centers. Simply stated, the Federal Government has limited influence in establishing infrastructure capabilities in individual centers and must rely instead on local decision makers.

The majority of fusion centers are used almost exclusively for law enforcement purposes. Due to 28 CFR regulations on how law enforcement information can be shared, fusion centers do not consistently engage owners and operators or share information with the private sector. In turn, a barrier to the sharing of private-sector information with fusion centers is the possible public release of the information through State “sunshine laws.” In briefings from legal experts, the NIAC learned that States have their own versions of FOIA and FACA. These “sunshine laws,” which include both open record laws and open meeting laws, vary greatly. Unless the information specifically is exempted under the State sunshine law, the information can be obtained by the public. Exemption clauses in State legislation are complex; and there are many different answers, depending on the individual State. To protect themselves, companies may be reluctant to share sensitive information in the fusion center environment. This includes not only vulnerability information but also suspicious activity reporting.

Appendix M reviews fusion center interactions with private sector owners and operators. Of 72 current fusion centers, eight are identified as success stores in infrastructure protection. There are the Arizona Counter Terrorism Intelligence Center, Boston Regional Intelligence Center, Dallas Fusion Center, Michigan Intelligence Operations Center, New York Police Department Real Time Crime Center, Northern California Regional Intelligence Center, South Nevada Counter Terrorism Center, and West Virginia Intelligence Fusion Center.

[20] The following description is based on I&A briefings to the NIAC in March and August 2011.

4.0 Recommendations

The need for effective information sharing between the public and private sectors has been a reoccurring finding in several NIAC studies and was the primary focus of our 2006 study on *Public-Private Intelligence Sharing.* Through these studies we have come to better understand the underlying issues and mechanisms that make information sharing succeed or fail. Our current study—the most exhaustive yet—reveals the complex ways information is gathered, analyzed, packaged, and shared among the owners and operators of critical infrastructure, and the structures and rules that govern how distinct types of information are shared with individuals at various levels within different types of organizations. Indeed, the challenge is daunting and the fixes are not simple. Yet we believe that understanding and accommodating the distinct information needs of the Intelligence Community, law enforcement, and critical infrastructure owners and operators is paramount to reducing risks to our Nation's critical infrastructure.

In developing our recommendations, we recognized the need to address the root causes that inhibit effective information sharing, as well as the many symptoms that lead to information sharing breakdowns between the public and private sectors. Breakdowns can occur when roles and missions are misunderstood, expectations are misaligned, or sensitive information is misused. Such breakdowns erode trust and are counterproductive to critical infrastructure protection and resilience. Therefore, our recommendations address each of the essential components of a complex information sharing system: authority and policy, implementation of authority, leveraging partner capabilities, information content, and information delivery, with separate topic areas on counterintelligence/counterterrorism and fusion centers.

Our overarching recommendation is that the Administration **should clearly and strongly assert the role and priority of critical infrastructure protection and resilience to National security, economic growth, and the well being of our citizens.** This is particularly important in light of emerging cyber risks, the growing sector interdependencies that affect business continuity, and ongoing criminal or terrorist threats to the Nation. Without this foundation, we believe it will be hard to accelerate effective bi-directional engagement that leverages the full capabilities of public and private partners across the entire intelligence cycle.

Recommendations	
Authority & Policy	**1. Assert the Priority of Infrastructure Protection and Resilience in National Security**
Implementation of Authority	**2. Improve the Implementation and Accountability of Existing Authorities**
Leveraging Partner Capabilities to Reduce Risk	**3. Improve Information Content by Leveraging Partner Capabilities**
Information Content	**4. Improve the Value of Information Products to Industry Risk-Management Practices**
Information Delivery	**5. Build Accepted Practices for Timely Information Delivery**
Counterterrorism	**6. Capitalize on Private Sector Capabilities for Counterterrorism Solutions**
Fusion Centers	**7. Enhance Fusion Center Capabilities as One Mechanism for Sharing**

4.1 Assert the Priority of Infrastructure Protection and Resilience in National Security

While the White House clearly recognizes the critical infrastructure protection imperative, it should vigorously affirm the criticality of infrastructure protection and resilience to our Nations' security and our citizen's well being through policy emphasis that drives action. Through a Presidential Policy Directive or other policy mechanism, the White House should achieve the following:

a. Direct all branches of the Federal Government to weigh issues of harm to sectors as they execute their missions. The continuity of sectors and their critical importance to the economic well being of the country should be weighed against needs of law enforcement, intelligence collection, and other high-priority missions.

b. Direct the Federal Intelligence Community to consider infrastructure protection and resilience as a national priority, to collect infrastructure intelligence needs, and to prepare a National Intelligence Estimate to evaluate terrorist targets in the 18 critical infrastructure sectors and assess vulnerability to such attacks, including cross-sector interdependencies and risks.

c. Direct that that DHS and the Office of the Director of National Intelligence, in collaboration with other members of the U.S. Intelligence Community and the Sector-Specific Agencies, prepare a quadrennial report on the state of intelligence information sharing for infrastructure protection and resilience.

In our 2006 study on intelligence information sharing, the Council recommended steps to improve key aspects of intelligence coordination between the public and private sectors, including actions to ensure the right decisionmakers receive information in a timely manner. This includes trusted communications between senior executives in government and private companies that own and operate critical infrastructure during a major crisis. In our 2008 study, *Critical Infrastructure Partnership Strategic Assessment,* we recommended that senior leadership engagement in and commitment to the partnership be strengthened in both government and industry. This includes the adoption of a self-scalable sector engagement model that builds trust among peers at the executive and operational levels.

Building on our 2006 and 2008 studies, we recommend that the White House reinforce the complementary role of public and private partners in *operational planning* for major threats and disasters, balancing the current focus on strategic planning. It should employ current partnership mechanisms—or establish a new formal mechanism if appropriate—for senior executives in the private sector to engage their government counterparts to facilitate a truly national approach that *leverages public-private resources* for large-scale, persistent threats.

4.2 Improve the Implementation and Accountability of Existing Authorities

The implementation of existing DHS authority reflects an early stage of maturity. The NIAC recommends five specific actions to improve performance and accountability and help mature DHS's role as a member of the Federal Intelligence Community:

a. The Office of the Director of National Intelligence (ODNI) should assist DHS in meeting its mission requirements by helping to specify, develop and/or modify, and assess the implementation of the programs and processes necessary to share intelligence information with the private sector, specifically information developed by other members of the Intelligence Community.

- Jointly with private sector partners, DHS should investigate ways to improve the fusion of threat, vulnerability, and consequence information to better evaluate the risk of emerging terrorist and criminal trends and improve prevention and mitigation measures. DHS should examine the use of Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) or a similar model as a mechanism to consider a broader range of sector/scenario planning and analysis.
- DHS should examine the balance of HITRAC's priorities between infrastructure protection and other missions. If HITRAC cannot serve critical infrastructure protection as a primary mission, DHS should consider developing a similar mechanism that 1) has infrastructure protection as its main priority, and 2) recognizes and integrates the information sharing capabilities that private sector owners and operators offer. In at least one critical sector, a private industry analyst has been integrated into HITRAC. We applaud this model and believe it could be replicated in other sectors.
- DHS should examine existing mechanisms for information sharing with the private sector and specifically attempt to simplify engagement pathways and eliminate information sharing redundancy.
- DHS should exercise existing mechanisms within the National Security Staff as an objective adjudicator when disagreements arise with other intelligence agencies over whether information has critical infrastructure protection implications and should be shared with the private sector.
  - DHS should aim to balance law enforcement's investigative needs and the protection of intelligence sources and methods with the need to share timely, actionable threat information with private sector.
  - Law enforcement investigators and intelligence agencies should consider the critical infrastructure implications of an event and work with DHS to share valuable information with the private sector while protecting their mission-specific concerns.
- ODNI and DHS should create incentives and opportunities for analysts to increase their critical infrastructure knowledge through personnel growth and career development.
  - ODNI should establish personnel performance incentives that encourage government analysts to design products and information that make the sector more secure.
  - ODNI and DHS should provide rotational assignment opportunities for analysts to gain experience in another agency or subject matter.
- DHS should develop a coordinated national program, specifically for critical infrastructure, that targets the identification, prevention, and mitigation of the trans-national threat of cyber attacks.
  - DHS, working with the SCCs and GCCs, that better identifies, characterizes, and prioritizes the cyber threats to the Nation's infrastructure.
  - DHS should develop a framework to provide standardized risk management guidance to aid companies, especially small and mid-sized businesses, to better prepare for and mitigate against cyber threats.
  - DHS should develop an aggressive outreach and awareness program to emphasize the growing cyber threat and the consequence to infrastructure business continuity of not recognizing and planning for these threats.

b. DHS should reexamine the rationale for, and effectiveness of, the DHS organizational structure of risk management functions for critical infrastructures with respect to the original intent of the

Homeland Security Act of 2002. This includes the organizational separation of threat analysis (in the Office of Intelligence and Analysis) from vulnerability and consequence analysis (in the Office of Infrastructure Protection).

- The public and private sectors use an established risk management strategy that leverages information from multiple sources to identify potential threats, evaluate vulnerabilities, and estimate consequences. This comprehensive risk picture enables owners and operators to prioritize the best security measures for their assets.

c. DHS, with the guidance and aid of ODNI, should establish core teams of 3-4 intelligence specialists for each sector, as well as a team that focuses on cross-sector information issues. These specialists should 1) be drawn from the members of the Federal Intelligence Community, 2) have expertise in both intelligence processes and sector business and risk-management processes, and 3) be responsible for fusing varied intelligence information streams into products useful for owner/operator planning and decision making.

- Each core team should operate at the National level but work with Sector-Specific Agencies (SSAs) and Sector Coordinating Councils (SCCs) to deliver the right information to owners and operators in specific regions or subsectors.
- A critical function of each team should be to inform the Intelligence Community of sector-specific information requirements, and advocate for these needs to collect and analyze actionable information products for sector customers. The team should serve as a bridge between partners in the private sector and the Intelligence Community, providing a critical feedback loop to improve the linkage between requirements and results.
- Sector-specific analysts should routinely meet with a small group of sector subject matter experts, such as a work group established by the Sector Coordinating Council (SCC) to garner feedback on intelligence needs and products.

d. ODNI should examine the complex relationships and rules for information sharing with the specific goal of reducing ambiguity and simplifying engagement points and processes.

e. Building on the roles and responsibilities defined in Homeland Security Presidential Directive 7, the President should define the specific functions, expected outcomes, and accountability measures for Sector-Specific Agencies (SSAs), and the SSAs should be given sufficient authority and capability to successfully execute these functions. To be most effective, SSAs should have:

- Infrastructure protection and resilience as their sole mission;
- The capability to operate as an effective interface for the bi-directional sharing of intelligence information, including working with their respective SCC in determining sector intelligence information needs and sharing them with the Federal Intelligence Community;
- A proactive role in understanding the capabilities of critical infrastructure owners/operators and integrating them with Federal partner capabilities; and
- Discrete budget authority and experienced, capable personnel commensurate with this mission.

4.3 Improve Information Content by Leveraging Partner Capabilities

To ensure that the Federal Government and the private sector can work effectively as partners in intelligence requirements definition, collection, analysis, and dissemination, the NIAC recommends that DHS work with each Sector-Specific Agency to implement, for all 18 critical infrastructure sectors, a robust intelligence requirements process that 1) meets the information needs of owners and operators, 2) delivers these requirements to appropriate elements of the Intelligence Community, 3) is consistent with existing Intelligence Community processes, and 4) supports advocacy for critical infrastructure priority within the Intelligence Community. This process should include the following elements:

- SSAs should work closely with individual Sector Coordinating Councils to lead the development sector-specific intelligence requirements. These requirements should be reviewed and updated at appropriate points to reflect changes in the sector's risk environment.
- DHS should aggressively advocate that that these requirements are integrated into the national intelligence collection requirements process.
- DHS should continue to apply the Critical Infrastructure and Key Resources Information Sharing Environment construct as a useful framework for organizing intelligence information sharing among diverse partners. This should:
    - Focus on linking the mission-based capabilities of public and private partners;
    - Promote the use of open-source information sources and analysis from all partners, thus building on contributions by the private sector as valuable resources for intelligence and analysis; and
    - Conduct an aggressive outreach and awareness campaign on the ISE purpose and capability to the sectors and other partners.
- DHS should streamline the process for providing private sector security clearances through the Private Sector Security Clearance Program (PSSCP), and develop opportunities for departing government personnel to keep or easily renew clearances when moving to key security positions in critical infrastructure companies.
- To support these requirements, the NIAC recommends that DHS develop a more robust and timely analysis capability that *leverages knowledgeable personnel and enhanced analytical resources* for each critical infrastructure sector to support sector-specific needs, business models, and risk-management processes. DHS should leverage commercially-available tools and techniques to provide capabilities for *predictive intelligence* for critical infrastructure protection. This process should include the following elements:
    - Review all existing government data bases and analytic tools to ensure that they are sufficiently up-to-date, have current software updates and are fully functional.
    - Establish the means to link and/or fuse multiple infrastructure databases in order to correlate relevant information and deliver warnings and recommended actions.
    - Promote the use of open-source information sources, analysis, and additional analytic tools available in the commercial market.
    - Support the development and more extensive use of tools such as predictive analytics and tabletop exercises that support the private sector's ability to actively improve their risk reduction measures.
    - Examine the use of existing analytic tools within the HITRAC program for potential use across a broader range of sector/scenario planning and analysis focused expressly on the information needed by private sector owner/operators.

4.4 Improve the Value of Information Products to Industry Risk-Management Practices

To ensure that the types of intelligence information used for protection and resilience are shared among partners, the NIAC recommends that the Office of the Director of National Intelligence, working jointly with DHS, establish new intelligence dissemination product formats to create tailored and practical products that help owners and operators protect assets and improve business continuity. DHS and its Federal intelligence partners should supplement classified threat briefings with unclassified reports that can be readily and broadly shared. The following elements will be critical:

- Products should include “traditional” finished products as well as relevant fragmentary data and information that may be valuable to the private sector.
- DHS should provide clear guidance to the private sector on how to properly handle unclassified but protected information, such as For Official Use Only information, based upon the Executive Order 13556 of November 4, 2010 on “Controlled Unclassified Information.”

4.5 Build Accepted Practices for Timely Information Delivery

All Federal mechanisms for sharing intelligence information should be examined with the goal of simplifying pathways, eliminating redundancy, and ensuring consistency of the information delivered. DHS should collaborate with the private sector to 1) identify critical infrastructure intelligence information sharing pathways and, 2) establish sector-specific intelligence information sharing protocols with the specific goal of improving timeliness. DHS and the Sector-Specific Agencies should work with the Sector Coordinating Councils to create formal networks of private-sector chief security officers and site security managers that will be used to facilitate timely, bi-directional public-private intelligence information sharing. DHS should consider the following to help achieve this goal:

- DHS should examine successful non-DHS mechanisms such as the Overseas Security Advisory Council (OSAC), and apply the lessons learned to improving DHS mechanisms.
- To ensure timely dissemination of classified information, the government should consider a program to provide classified cell phones to cleared security officers in critical infrastructure sector companies.
- DHS should examine and consolidate critical infrastructure intelligence information sharing pathways and mechanisms to eliminate conflicting information, reduce redundancies, and increase the efficiency, timeliness, and consistency of information sharing tools.
- DHS should continue and expand its pilot program with the Banking and Finance Sector to develop the Government Information Sharing Framework (GISF) to improve the information sharing of threat and attack data between government and industry.

In addition, DHS should support and reinforce the Homeland Security Information Network – Critical Sectors (HSIN-CS) implementation to achieve three desired outcomes: 1) sectors understand that they *are the customer* and their needs drive system requirements, 2) system implementation is based on and measured by *understanding and meeting these user needs*, and 3) system architecture takes advantage of state-of-the-art, commercially available tools for threat analysis in order to meet these needs in a timely manner. Appropriate senior-level management leadership and oversight must be provided to keep this goal on track. DHS should facilitate the use of HSIN-CS as a tool, building on success models such the HSIN-CS portal used by NICRIC. This development should include the following elements:

- Recognize the shortcomings expressed by the private sector (cumbersome, difficult to use, needing a push system rather than pull system to access information) and *implement* an action plan to remedy these issues.
- Educate potential users on the capabilities of HSIN, enabling them to take a proactive role in determining how the HSIN backbone of services can be used for specific sector needs.

- Engage the private sector (through the appropriate Sector Specific Agency and Sector Coordinating Council) to help guide requirements and design of HSIN-CS to make it most effective for them.
- Use up-to-date technology platforms to take advantage of commercially available tools and techniques for data and information analysis.

4.6 Capitalize on Private Sector Capabilities for Counterterrorism Solutions

The Federal Government should capitalize on the information collection and analysis capabilities of private sector partners, and incorporate this knowledge base to improve existing products and processes. DHS should provide specific guidance on the most important areas of emerging counterterrorism information on which the sectors should focus, and update these areas on a regular basis as conditions dictate.

- DHS should also provide direct and timely feedback to the sectors on the effectiveness of the information they provide through Suspicious Activity Reporting and other means. This should be coordinated through the SSA where practical.

4.7 Enhance Fusion Center Capabilities as One Alternative Mechanism for Sharing

Where appropriate, DHS should guide fusion centers to establish an information sharing function with owners and operators as part of a critical infrastructure protection and resilience mission. We recognize that not all fusion centers align with critical infrastructure assets, or operate under State laws and policy that allow or encourage the integration of critical infrastructure information. Regardless, DHS should support—through funding, personnel, training, technology, and analytic tools—the development of an infrastructure protection and resilience capability that *could stand alone or be integrated* within fusion centers to facilitate the flow of intelligence information to and from the private sector, while ensuring information protection and addressing privacy concerns. The grant process for fusion center funding should specifically require an infrastructure protection mission if fusion centers are to be broadly appropriate to that mission. To further provide support to fusion centers in meeting their critical infrastructure protection mission, DHS should provide the following:

- DHS should develop standard guidance to help fusion center operators understand private sector information protection and privacy concerns and their roles regarding information protection.
- DHS, in order to better support the four Critical Operational Capabilities (COCs)—receive, analyze, disseminate, and gather—for incorporating critical infrastructure into fusion center operations, should do the following:
  - Sponsor training and/or rotational assignments with fusion center analysts.
  - Assist fusion centers with developing analytic products to distribute to relevant sectors.
  - Assist fusion centers and their private sector partners in become active participants in the National Suspicious Activity Reporting (SAR) Initiative (NSI).
  - Develop fusion center-specific portals for facilitating a bi-directional flow of information between fusion centers and the private sector.
  - Overlay international or national intelligence with State, local, and regional information to help fusion centers develop timely and actionable intelligence products for their respective critical infrastructure partners.

  - Use grants and other funding mechanisms, specifically tied to the infrastructure protection mission, to encourage States to incorporate baseline CIP capabilities within their fusion centers.

Where this mission alignment does not take place, DHS should instead direct available critical infrastructure protection resources to an alternative approach *specifically designed with information sharing with private sector owners and operators as its goal.* If a grant process for fusion centers is used, it should specifically require an infrastructure protection mission and a process for sharing with the private sector.

Appendix A. Acknowledgements

NIAC Working Group Members

- Alfred R. Berkeley III (Co-Chair), Chairman, Pipeline Trading Systems, LLC
- Philip G. Heasley (Co-Chair), President and Chief Executive Officer, ACI Worldwide
- James B. Nicholson (Co-Chair), President and Chief Executive Officer, PVS Chemicals, Inc.
- Wesley Bush, Chairman, President and Chief Executive Officer, Northrop Grumman
- James A. Reid, President, CBRE Group, LLC – Eastern Division
- Michael J. Wallace, Former Vice-Chairman and COO, Constellation Energy

Study Group Members

- Joan Gehrke (Co-Chair), Special Projects Manager, PVS Chemicals, Inc.
- Robin Holliday (Co-Chair), Principal Professional Staff,
  Johns Hopkins University Applied Physics Laboratory
- Gerald Buckwalter, Vice President, Homeland Security, Northrop Grumman
- Dr. Antonio De Simone, National Security Analysis,
  Johns Hopkins University Applied Physics Laboratory
- Joseph Donovan, Senior Vice President, Beacon Capital Partners, LLC
- Dr. John Gannon, President, Intelligence and Security Business, BAE Systems
- Ed Goetz, Executive Director, Corporate and Information Security, Constellation Energy
- Ronald Hicks, Director of Corporate Security, Anadarko Petroleum Corporation
- Dr. Erin Mullen, Assistant Vice President, RX Response, PhRMA
- Bill Muston, Executive Manager, Research & Development,
  Oncor Electric Delivery Company, LLC
- Nitin Natarajan, Coordinating Director, HHS/ASPR/OPEO, U.S. Department of Health and Human Services
- Jim Rosenbluth, Managing Director, Crisis Management, Cushman &Wakefield, Inc.
- Timothy Scott, Chief Security Officer, Dow Chemical Company
- Stanley Szemborski, Vice President of Corporate Strategy, Northrop Grumman

Case Study Leads

Banking and Finance Sector

- Alfred R. Berkeley III, Chairman, Pipeline Trading Systems, LLC
- Philip G. Heasley, President and Chief Executive Officer, ACI Worldwide

Chemical Sector

- Joan Gehrke, Special Projects Manager, PVS Chemicals, Inc.
- Timothy Scott, Chief Security Officer, Dow Chemical Company

Commercial Facilities Sector

- James A. Reid, President, CBRE Group, LLC – Eastern Division
- Joseph Donovan, Senior Vice President, Beacon Capital Partners, LLC

Oil and Natural Gas Sector (Energy)

- Jay Montgomery, Director-Security, Kinder Morgan
- Raymond Reese, Corporate Health Safety and Security Leader, Colonial Pipeline Company

Healthcare and Public Health Sector

- Dr. Erin Mullen, Assistant Vice President, RX Response, PhRMA
- Nitin Natarajan, Coordinating Director, HHS/ASPR/OPEO, U.S. Department of Health and Human Services

Subject Matter Experts

- Rod Nydam, Founder, Nydam Law
- Neill Sciarrone, Senior Director, Strategy and Planning, BAE Systems
- Evan D. Wolff, Partner, Hunton & Williams

Support Staff

- Jim Carey, Energetics Incorporated
- Jack Eisenhauer, Nexight Group LLC
- Kate Finnerty, Energetics Incorporated
- Martin Lasater, Energetics Incorporated
- Jennifer Rinaldi, Energetics Incorporated
- Marc Sigrist, Energetics Incorporated
- Lindsay Kishter, Nexight Group LLC
- Robert Briggs, SRA International
- Adrienne Barge, Vet-Fed Resources

Appendix B. Case Study: Banking and Finance Sector

Table of Contents

1.0 Introduction

The Banking and Finance Sector has a well-established history of collaborative efforts to share threat and risk intelligence amongst themselves and with various government agencies. As the sector is subject to multiple Federal, State, and international regulations, it continually works with its regulatory agencies to develop better information-sharing relationships.

In the face of increasingly sophisticated threats, particularly cyber threats, the Banking and Finance Sector requires intelligence that provides *timely*, *predictive* information to help identify potential perpetrators, characterize likely threat modes, and prepare to mitigate damage. The need for strengthened intelligence-sharing mechanisms to support this, however, must be balanced with concerns over liability, confidentiality, and control of proprietary information.

Current efforts to improve the sharing of intelligence information within the sector include: enhanced coordination of crisis response through timely dissemination of critical information within the sector and among sector stakeholders; improved communications with the United States Computer Emergency Readiness Team (US-CERT), the U.S. Intelligence Community, and the law enforcement community to share information on cyber security threats; development of strategies to reduce the potential impact of cyber threats; and educational and awareness programs to further enhance communications within the sector.

2.0 Sector Profile

As a critical service provider to many other critical U.S. sectors, the Banking and Finance Sector must maintain essential operations at all times, even during national emergencies. It is a millisecond sector—that is, it fundamentally relies on instantaneous transactions—to facilitate national and world economic activity by working within a complex and extensive supply chain across both public and private organizations in major markets around the world. Assets in the Banking and Finance Sector total nearly $50 trillion. The sector provides four broad types of services:

1. Deposit and payment systems and products ($12 trillion in assets; 17,000 depository institutions)
2. Credit and liquidity products ($14 trillion in assets; many thousands of credit and financing institutions)
3. Investment products ($18 trillion in assets; 15,000 providers of investment products)
4. Risk-transfer products ($6 trillion in assets; 8,500 providers of risk-transfer products)

Nearly all of these services are conducted electronically with an extensive network of national and international entities, primarily through privately owned infrastructure. Though it is the backbone of nearly every other critical sector, the Banking and Finance Sector relies heavily on the Energy, Information Technology, Transportation Systems, and Communications Sectors for critical operations. As sector services and products are so expansive, there is a critical focus on securing and mitigating threats to processes. In the recent past, attacks have primarily been both cyber and criminal in nature, such as data breaches aimed at gaining credit card and account information for illegal financial gain.

Security Characteristics

Addressing cyber security threats, whether criminal or terrorist, is paramount. The expanding global economy and global financial systems require reliable, real-time electronic connections for even the most highly sensitive data. Most global financial firms operate on multiple continents and require technology support teams in one country to have access to operations elsewhere in the world. Financial firms also need to access e-mail, storage, and revenue-producing applications across major financial hubs to support mission-critical functions. Moving this data around the world depends on a broad suite of communications, hardware, and software applications. Firms depend upon a secure and resilient communications infrastructure to perform essential global financial services functions, including payments, clearing and settlement, and foreign exchange.

Of particular concern to the sector are advanced cyber threats, which are sophisticated, highly organized, often state-sponsored, and specifically directed against networks and computer systems containing highly sensitive information.[21] Detecting, protecting against, and responding to these kinds of threats require even closer, cooperative relationships between private sector financial institutions and relevant government entities.[22] Neither the private sector nor the government alone can successfully manage these cyber intrusions.[23] Sector security specialists note a shift in the targets of sophisticated cyber attacks, which often now focus on smaller companies that cannot afford the same level of protection or access to intelligence sources that larger companies can. Because the sector is highly interconnected, criminals can often get the information or access they want by targeting smaller companies and in turn accessing the electronic networks that tie them to larger institutions. Figure BF-1 provides examples of recent cyber attacks targeting financial institutions.

History of Regulation

The Banking and Finance Sector has long and embedded relationships with Federal, State, and local governments, stemming from over 150 years of financial regulation and reporting requirements. The vital role the Banking and Finance Sector has always played in the economic health of both the national and the global economy has necessitated sector compliance with multiple Federal, State, and international regulations. These regulations form a complex regime of oversight structures that monitor operational, financial, and technological systems. These authorities most notably include the U.S. Securities and Exchange Commission (SEC), the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve, and the Office of the Comptroller of Currency. All conduct examinations of financial systems to address information security, business continuity, vendor management, and other operational risks. The Banking and Finance Sector works with its regulatory agencies to develop better information-sharing relationships, specifically enhancing progress through research, exercises, protective measures, and identification of emerging threats.

[21] For a single such threat, spanning five years and involving more than 70 global companies, see McAfee White Paper, “Revealed: Operation Shady RAT,” 2011, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

[22] For a discussion of these challenges scenarios, see National Cyber Defense Financial Services Workshop Report, “Helping Form a Sound Investment Strategy to Defend against Strategic Attack on Financial Services,” October 28-29, 2010, hosted by BITS, FSTC, and Financial Services Roundtable and sponsored by the National Science Foundation and DHS S&T. Report published February 4, 2010, http://ncdi.cisr.us/FI_Workshop_Report_100204.pdf.

[23] For an overview of the cyber-security challenge to the nation, see GAO Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, “Cyber Security: Continued Attention Needed to Protect Our Nation’s Critical Infrastructure,” GAO-11-865T, July 26, 2011, http://www.gao.gov/new.items/d11865t.pdf.

Figure BF-1. Examples of Cyber Crime in the Banking and Finance Sector

Attempts to breach financial sector computers and networks occur frequently and have origins from around the world. A few examples of recent cyber crimes:

- October 2010—Zeus malware targeted U.S. computers, stealing ~$70 million. Zeus malware (Zbot) was detected in 2007, the FBI announced arrests in October 2010, and the source code was published in May 2011. The malware enabled hackers to steal FTP, e-mail, and online banking passwords for financial gain. The FBI announced that the malware enabled hackers to steal around $70 million as a result of hacking into U.S. computers. Source: "More Than 100 Arrests, as FBI Uncovers Cyber Crime Ring," *BBC*, October 1, 2010, http://www.bbc.co.uk/news/world-us-canada-11457611.

- January 2011—European Union carbon-trading markets penetrated by hackers, stealing >$9 million. More than $9 million worth of greenhouse-gas emissions permits were stolen from the Czech Republic electricity and carbon-trading registry and transferred to accounts in other countries. The European Commission estimated that roughly 2 million allowances (worth almost $40 million) were illegally transferred out of accounts in three separate attacks. European Union allowances "permit energy companies and industrial factories to trade their pollution permits by buying and selling allowances allocated by their government." Source: Elinor Mills, "Hackers Hit Market for Carbon Trading," TechTalk, January 21, 2011, http://www.cbsnews.com/8301-501465_162-20029253-501465.html.

- March 2011—RSA breach extracted information on SecureID products. RSA SecureID tokens, used by many public and private sector companies for two-factor authentication, suffered a cyber attack in March 2011. This breach helped enable the Lockheed Martin, Northrop Grumman Corp. and L-3 Communications attacks that occurred in May 2011. Source: Art Coviello, "Open Letter to RSA Customers," RSA, 2011, http://www.rsa.com/node.aspx?id=3872; William Jackson, "More Cyberattacks Reported; RSA Tokens Likely Involved," Washington Technology, June 1, 2011, http://washingtontechnology.com/articles/2011/06/01/defense-contractors-l3-lockheed-hacked.aspx.

- June 2011—Hackers viewed Citigroup customer account information. Citigroup announced a security breach in June 2011, potentially affecting 200,000 credit card customers. The cyber attack enabled hackers to view credit card customer account information, including customers' names, account numbers, and contact information. Source: Stanglin, Douglas, "Citigroup says hackers gained access to some credit card data," June 19, 2011, *USA Today*, http://content.usatoday.com/communities/ondeadline/post/2011/06/citigroup-says-hackers-gained-access-to-some-credit-card-data/1.

- June 2011—Hackers stole credit and debit card numbers. The U.S. Secret Service reported to Congress in 2011 that its investigation of "carding websites" involved in hacking major U.S. retailers had uncovered instances of theft of more than 40 million credit and debit card numbers. Source: *Hacked Off: Helping Law Enforcement Protect Private Financial Information, Before the House Committee on Financial Services,* 112th Cong. (June 29, 2011) (testimony of Assistant Director A.T. Smith, Office of Investigations, U.S. Secret Service), http://www.dhs.gov/ynews/testimony/20110629-smith-protecting-financial-information.shtm.

Many laws also govern the nature and extent of information sharing between the sector and its various regulatory agencies. The most notable statutory authorities at the Federal level include:[24]

- Commodity Exchange Act (7 U.S.C. § 1, et seq.)
- Bank Service Company Act (12 U.S.C. § 1861, et seq.)
- Federal Reserve Act (12 U.S.C. § 248(a))
- Bank Holding Act of 1956 (12 U.S.C. § 1844(c))
- Federal Credit Union Act (12 U.S.C. § 1751, et seq.)

[24] For an extensive list of authorities governing the Sector, see U.S. Department of Homeland Security and U.S. Department of Treasury, *Banking and Finance Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan* (May 2007), http://www.cfr.org/economics/banking-finance-critical-infrastructure-key-resources-sector-specific-plan-input-national-infrastructure-protection-plan/p14637.

- Security Exchange Act of 1934 (15 U.S.C. 78a, et seq.)
- Securities Investor Protection Act of 1970 (15 U.S.C. 78aaa, et seq.)

The Banking and Finance Sector functions globally, and accordingly participates in several self-regulatory organizations—such as the Municipal Securities Rulemaking Board (MSRB), the Financial Industry Regulatory Authority (FIRA), and the National Future Chicago Mercantile Exchange (CME)—to oversee industry practices related to security and resilience for both domestic and overseas operations. The sector also reaches out to international organizations and governments to enable greater communication of emerging threats and to improve emergency preparedness of critical financial institutions.

3.0 Banking and Finance Sector Information Sharing Framework and Processes

The Banking and Finance Sector has a complex network of partners and stakeholders in intelligence information sharing, including regulatory agencies, government and industry organizations supporting critical infrastructure protection, industry associations, intelligence agencies, and law enforcement. Interviews with security specialists across the Banking and Finance Sector, supported by open-source research, formed the following examination of the information sharing relationships within the sector, the mechanisms and tools for sharing threat information, and the effectiveness of coordination among those stakeholders and mechanisms to get the right information to the right people in time to take action.

Banking and Finance Sector Information Sharing Relationships

The Banking and Finance Sector leverages robust and effective information sharing relationships using the National Infrastructure Protection Plan (NIPP) sector partnership model. The Sector-Specific Agency (SSA) for the sector is the Department of the Treasury, which collaborates with all relevant Federal agencies and State and local governments to coordinate risk management strategies with the sector. The Department of the Treasury also serves as a primary regulatory body for the sector.

The sector coordinates information sharing primarily through four private and public-sector organizations: the Financial Services Sector Coordinating Council (FSSCC);[25] the Financial Services Information Sharing Analysis Center (FS-ISAC);[26] the Regional Partnership Council Financial Industry Resilience, Security, and Teamwork (RPC*first*);[27] and the Financial and Banking Information Infrastructure Committee (FBIIC).[28] Figure BF-2 provides an overview of the roles of these organizations.

Figure BF-2. Roles of Private and Public Institutions for Banking & Finance Sector Information Sharing and Collaboration

Institution	Description	Role

[25] Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, *Annual Report 2009* (Financial Services Sector Coordinating Council, January 2010), https://www.fsscc.org/fsscc/reports/2010/FSSCC-2009AnnualReport.pdf; Financial Services Sector Coordinating Council home page, 2008, https://www.fsscc.org/fsscc/default.jsp.

[26] For a description of the FS-ISAC, see "About the FS-ISAC," Financial Services Information Sharing and Analysis Center, 2011, http://www.fsisac.com/about/.

[27] "About RPDfirst," RPCfirst, 2011, http://www.rpcfirst.org/. For a list of regional members, see "Partnership Members," RPCfirst, 2011, http://www.rpcfirst.org/partnerships/default.asp.

[28] Financial Banking and Information Infrastructure Committee home page, updated April 1, 2010, http://www.fbiic.gov/. FBIIC maintains a very useful information sharing webpage at: http://www.fbiic.gov/whatsnew.htm.

Private Sector Organizations		
Financial Service Sector Coordinating Council (FSSCC)	The FSSCC fosters and facilitates the coordination of Sector-wide voluntary initiatives to improve critical infrastructure protection and homeland security. The organizations comprising the FSSCC hold the majority of the assets of the Sector and include financial institutions, trade associations, and regional partnerships.	Among its various missions, the FSSCC is especially focused on ensuring that the private sector entities comprising the Sector are coordinating and cooperating with government entities for critical infrastructure protection and homeland security issues, including the sharing of information and knowledge.
Financial Services Information Sharing Analysis Center (FS-ISAC)	The FS-ISAC is one of the oldest private information-sharing initiatives in the U.S. It was established as the financial sector response to the requirements of Presidential Decision Directive 63 (Protecting America's Critical Infrastructures) in May 1998. The FS-ISAC is a member-supported organization, with memberships having varying levels of benefits. Currently, there are 1,961 direct links from the FS-ISAC to financial institutions and an estimated 11,000 indirect links through member associations.	The principal mission of the FS-ISAC is to coordinate information sharing within the Sector, including cyber and physical threat information, vulnerability and incident alerts, and communications during an emergency. The FS-ISAC is the recognized conduit by which all major stakeholders, including the Department of the Treasury and the FSSCC and FBIIC, share information with the private sector.
Regional Partnership Council Financial Industry Resilience, Security, and Teamwork (RPC*first*)	RPC*first* focuses on coordination among the major regional banking and finance organizations around the country. Regional partnerships within the Sector began to form with ChicagoFIRST in 2003. Currently, there are 24 regional partnerships, representing all parts of the United States.	The mission of RPC*first* is to ensure that the coalition of regional partnerships within the Sector share lessons learned relating to coordination with local and State governments; participate in national homeland security policy making through participation in the FSSCC; and leverage their relationships with one another to engage in business continuity and homeland security efforts effectively and efficiently.
Financial and Banking Information Infrastructure Committee (FBIIC)	Headed by the Department of the Treasury, the Sector-Specific Agency (SSA) for the Sector, and comprised of member agencies and Sector regulators. The financial regulators work together through the FBIIC to coordinate efforts with respect to critical infrastructure protection issues.	The FBIIC's role is to coordinate the efforts of Federal and State financial regulators with respect to critical infrastructure issues, including preparation for and response to cyber or physical attacks against the financial system or indirect attacks or events that may impact the Sector.

The FSSCC and FS-ISAC are the primary agents through which private sector firms can share information on threats, vulnerabilities, and incidents. These organizations have developed crisis-management protocols that use the FS-ISAC mechanisms to rapidly share intelligence-derived information with private sector partners. The FS-ISAC is a nonprofit organization that provides a forum for collaboration on security threats and risks facing the sector. The FS-ISAC partners with government intelligence, regulatory, and law enforcement agencies to better enable information sharing between the public and private sectors.

The FS-ISAC receives intelligence information from the Federal Government at Top Secret, Secret, and unclassified levels. In addition to DHS, the FS-ISAC works with other Federal organizations including the National Security Agency (NSA), the Central Intelligence Agency (CIA), the U.S. Secret Service (USSS), and the Federal Bureau of Investigation (FBI). The ISAC receives strategic and tactical information, as well as law enforcement and national/homeland security information, with a focus on organized crime against financial institutions.

Information provided by the FS-ISAC to its members includes analysis and recommended solutions from leading industry experts. Members join the FS-ISAC because of the strong reputation of the organization and its willingness to develop tailored processes and products for security information sharing within subsectors of the financial services industry. One example of an FS-ISAC initiative is the Payments Process Information Sharing Council, described in Figure BF-3.

In the sector, Sector Specialists play an important role in acting as a liaison between the private sector and various programs in the government. The private sector can approach the two financial Sector Specialists, one from the FDIC and the other from the USSS, and request to be connected with the government entity involved in a particular issue, and the Sector Specialist will facilitate the necessary introductions for the effective exchange of information to take place.

Coordination with interdependent sectors occurs primarily through information-sharing bodies such as the Partnership for Critical Infrastructure Security (PCIS) and the DHS National Infrastructure Coordination Center (NICC).

The Banking and Finance Sector relies heavily on private sector security companies to not only provide physical and cyber security, but to share threat and attack information. For example, VeriSign provides valuable lessons learned from security breaches within the sector, such as the Distributed Denial of Service (DDoS) attacks of July 2009.[29] VeriSign also offers the sector the iDefense Security Intelligent Service that is intended to provide security executives with timely, accurate, and actionable cyber intelligence with specific emphasis on vulnerabilities, malicious code, and global threats. Utilizing services such as these enables the sector to develop and update security strategies and mitigation techniques that, in turn, enable business continuity and protect sensitive information from being stolen or misused.

Figure BF-3. Payments Processing Information Sharing Council

The FS-ISAC is developing the Payments Processing Information Sharing Council (PPISC), a mechanism for the payments industry to share information about fraud, threats, and vulnerabilities, as well as mitigation practices and lessons learned.

William B. Nelson, president and CEO of the FS-ISAC, noted, "Data security in the payments processing supply chain is critically important – and this industry has unique needs. By forming this council as part of FS-ISAC, we can be very effective in quickly focusing on these needs and expediting the disclosure of information and risk-mitigation strategies which are crucial in the fight against cyber criminals."

Source: FS ISAC, "Payments Processing Information Sharing Council Forms to Foster Information Sharing among Payments Processors," March 23 2009, http://www.fsisac.com/files/public/db/p173.pdf, accessed January 2011.

Current Efforts to Enhance Information Sharing

The Banking and Finance Sector is working closely with these partners to improve coordination on intelligence and information sharing. Current efforts include:

- Refinement and application of the Banking and Finance Sector threat matrix.[30] This matrix enables sector partners to deter, mitigate, and respond to significant sector threats, incidents, and vulnerabilities by identifying critical assets, establishing infrastructure priorities, and developing effective protection and resilience strategies.

[29] VeriSign Intelligence Operations Team, "Distributed Denial of Service (DDoS) Attacks: An Overview and an Analysis," June 4 2010, http://www.fsisac.com/files/public/db/p244.pdf, accessed April 2011.

[30] For information about the threat matrix, see Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, *Annual Report 2009* (Financial Services Sector Coordinating Council, January 2010), 16 ff, https://www.fsscc.org/fsscc/reports/2010/FSSCC-2009AnnualReport.pdf.

- Improved communication with the U.S. Computer Emergency Readiness Team (US-CERT), the U.S. intelligence community, and the law enforcement community to share information on cyber security threats and to develop strategies to reduce the potential impact of such threats.
- Strengthened coordination with DHS to sponsor security clearances for need-to-know private sector personnel to facilitate the sharing of classified information.

Figure BF-4. U.S. Secret Service ECTFs and CIS

Congress in the USA PATRIOT Act of 2001 (Public Law 107-56) directed the USSS to establish a nationwide network of Electronic Crimes Task Forces (ECTFs) to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

Current membership in the 31 ECTFs includes 4,093 private sector partners; 2,495 law enforcement partners; and 366 academic partners.

CIS leverages technology and information obtained through private sector partnerships to monitor developing technologies and trends in the financial payments industry to enhance the Secret Service's capabilities to prevent and mitigate attacks against financial and other critical infrastructures.

The sector also has extensive information-sharing partnerships with intelligence agencies. The USSS plays a prominent role in combating cyber crime, maintaining a permanent presence at the National Cyber Investigative Joint Task Force. This task force serves as the coordination and integration center for the identification, mitigation, and neutralization of both criminal and national security threats against the United States.[31] Since 1995 the USSS has established 31 Electronic Crime Task Forces (ECTFs) around the country that hold monthly meetings with the private sector, academia, and local, State, and Federal law enforcement agencies to identify, outline, and mitigate potential cyber threats. The USSS also partners with the private sector in its Cyber Intelligence Section (CIS). Figure BF-4 provides a description of the ECTF and CIS programs. One example of a joint USSS effort with both the U.S. private sector and international partners is the *2011 Data Breach Investigations Report*, conducted by the Verizon RISK Team in cooperation with the USSS and the Dutch High Tech Crime Unit.[32]

In addition to its cooperation with the USSS, the sector works closely with the US-CERT, which produces and disseminates actionable cyber security threat information and mitigation strategies. The sector actively participates in the DHS Cross-Sector Cyber Security Working Group, which facilitates cyber security information sharing between the critical infrastructure sectors. DHS also sponsors cyber training that includes participation from organizations such as FSSCC, FS-ISAC, RPC*first*, USSS, and the FBI.

Both the public and private sector are taking steps to build active cyber security partnerships that address emerging issues, such as supply chain security and identity management. An example is the December 2, 2010 Memorandum of Understanding (MOU) between the FSSCC, the DHS Science and Technology Directorate (S&T), and the National Institute of Standards and Technology (NIST) of the Department of Commerce. The MOU is to leverage their respective expertise, research and

[31] For overviews of USSS protection of financial information, see *Cyber Security and Data Protection in the Financial Sector, Before the Senate Committee on Banking, Housing, and Urban Affairs*, 112th Cong. (June 21, 2011) (statement of Mr. Pablo A. Martinez, Deputy Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service), http://www.dhs.gov/ynews/testimony/20110621-martinez-cyber-crime.shtm; *Hacked Off: Helping Law Enforcement Protect Private Financial Information, Before the House Committee on Financial Services*, 112th Cong. (June 29, 2011) (testimony of Assistant Director A.T. Smith, Office of Investigations, U.S. Secret Service), http://www.dhs.gov/ynews/testimony/20110629-smith-protecting-financial-information.shtm.

[32] Verizon, *2011 Data Breach Investigations Report* (Verizon, 2011), http://www.secretservice.gov/Verizon_Data_Breach_2011.pdf.

development capabilities, and other resources to facilitate cyber security innovation, identify and overcome cyber security vulnerabilities, and develop more efficient and effective cyber security processes that benefit critical financial services functions and may benefit other critical infrastructures. It aims "to expedite the coordinated development and availability of collaborative research, development, and testing activities for cyber security technologies and processes based upon the Financial Services [Banking and Finance] Sector's needs."[33] Another example of a new partnership focused on cyber security is a pilot project launched in February 2010 between DHS, the Department of Defense (DoD), and the FS-ISAC to protect critical infrastructure within the sector by sharing actionable, sensitive information.[34]

4.0 Effectiveness of Information Sharing in the Banking and Finance Sector

The purpose of NIAC interviews with security specialists in the Banking and Finance Sector was to gauge the effectiveness of the information-sharing partnerships and mechanisms they use and evaluate where improvements could be made. The following describes the effectiveness of current procedures and details new capabilities that the sector sees as especially promising in strengthening information sharing between the government and private sector.

4.1 Issues on Bi-directional Information Sharing

While the sector believes that bi-directional information sharing with government is strong and steadily improving, interviews with sector subject matter experts pointed to several areas that needed improvement. These issues are described below.

The Information Shared is Primarily Reactive, not Predictive, in Nature

Most of the information being shared between government and the sector is criminal intrusion information, mainly about the technical attributes of intrusions that have already happened. What the sector wants to receive is information about threats before incidents occur, so efforts can be made to reduce the severity or impact of future attacks. This is an important paradigm shift from protecting against past events to strengthening the resilience of infrastructure to withstand future events. It is the main impetus behind the sector's support of wider use of predictive analytics (explained further in the following section).

Conflicting Missions from Multiple Information Sharing Stakeholders

Numerous government and intelligence agencies have a range of cyber security responsibilities, including protection from, response to, and investigation of cyber attacks. These multiple roles result in sometimes conflicting missions that can affect what intelligence is shared with the private sector and how they are able to act on it. In the now well-known NASDAQ hack, the law enforcement mission to investigate the attack and catch the criminals conflicted with other agencies' missions to share the

[33] "Partnership for Cyber-security Innovation," White House Office of Science and Technology Policy, December 6, 2010, http://www.whitehouse.gov/blog/2010/12/06/partnership-cybersecurity-innovation.

[34] *Examining the Cyber Threat to Critical Infrastructure and the American Economy, Before the United States House Committee on Homeland Security Subcommittee on Cyber Security, Infrastructure Protection, and Security Technologies*, 112th Cong. (March 16, 2011) (testimony of Deputy Under Secretary Philip Reitinger, National Protection and Programs Directorate), http://www.dhs.gov/ynews/testimony/testimony_1300283858976.shtm. For an overview of the Obama Administration's efforts to protect U.S. critical infrastructure from cyber attack, see *Protecting Cyberspace: Assessing the White House Proposal, Before the Senate Homeland Security and Governmental Affairs Committee*, 112th Cong. (May 23, 2011) (statement for the Record of Philip Reitinger, Deputy Under Secretary, National Protection and Programs Directorate) http://www.dhs.gov/ynews/testimony/testimony_1306166133258.shtm.

attack information extensively with the private sector to prevent continuing or additional attacks. This resulted in “continuing harm” to the private sector, as some companies were delayed in receiving the information and left vulnerable to attacks known by the government. Figure BF-5 provides more on the issue of continuing harm.

Figure BF-5. Balancing Law Enforcement and Critical Infrastructure Protection: The Issue of Continuing Harm

While a clear and growing concern in the sector is the compromise of business-critical information from cyber intrusions, an underlying concern is the potential for continuing harm after an intrusion is first discovered. This can occur when the law-enforcement mission to investigate the perpetrator(s) allows the intrusion to continue. One example was described by the Chairperson of the FSSCC in testimony before Congress on April 15, 2011.* The incident she described was an intrusion through the Director’s Desk web-facing service at NASDAQ OMX Group.**

She said: “An example of an incident where too much secrecy led to an increased exposure was the cyber attack on a major exchange, which was discovered by the exchange in October 2010. The exchange alerted its primary regulator and law enforcement. For a variety of reasons, including an investigation of the attack by law enforcement and intelligence agencies, information about the attack and its impact on other financial institutions was not disclosed to others in the financial services sector for 102 days. This 102-day period included year-end, when financial institutions close their books and prepare annual reports. This could have had an enormous impact on employees, stockholders, large and small, and the market as a whole. The lack of meaningful information for more than three months left the entire Sector unnecessarily vulnerable.”

Sources:

* Jane Carlin, before the Subcommittee on Cyber Security, Infrastructure Protection and Security Technologies of the Homeland Security Committee of the House of Representatives, April 15, 2011.

** Devlin Barrett, “Nasdaq Acknowledges Security Breach,” *Wall Street Journal*, February 6, 2011, http://online.wsj.com/article/SB10001424052748704843304576126370179332758.html.

Unclear Distinction between the Roles of the Commercial Facilities Sector and the Banking and Finance Sector for Property Management

Because many financial institutions are tenants within commercial facilities (which fall under the responsibility of the Commercial Facilities Sector), financial managers often look to the real estate owners and operators for physical protection. Several of those interviewed reported that their landlords received more timely and accurate physical threat information than they did. On other occasions, however, the landlord received no information about possible threats to the financial services tenant. The government agencies sharing threat information often do not understand the distinct protection responsibilities of the facility owner and facility occupant, and as a result, physical threat information may not get to the person capable of taking action against it.

Information Sharing Limited with Multinational Banks

One challenge for multinational banks is that their employees, and even executives, are not American citizens. U.S. banks may employ non-citizens in key positions, and foreign-chartered banks may have an even larger presence of non-U.S. citizen employees in critical security roles. This limits the ability of the Federal Government to share threat information, as laws restrict how it shares information with noncitizens. Financial institutions must establish alternate internal information-sharing processes to mitigate this issue.

CEOs and CFOs Lack Education on Cyber Threats

Interviewees reported several cases in which CEOs and CFOs were either not told of emerging cyber threats within their companies by their staff, or they did not place appropriate priority on the information given other risk-management considerations. The highest-ranking decision makers in corporations often do not attend the classified (or even unclassified) briefings given by the USSS, FBI, DHS, and other intelligence agencies. Cyber threats are complex and difficult to predict with certainty, or to examine the potential consequences beforehand. As a result, many chief executives lack a thorough understanding of the criticality of cyber threats that their companies now face. Physical threats are more easily quantified and understood, and most corporations routinely take measures to protect their facilities and personnel. Executive-level educational programs are needed to increase understanding of emerging cyber threats to the industry and enable the same proactive approach.

Regulatory Obstacles to the Sharing of Information

Many regulations including those providing necessary protections to sensitive information, can impede or slow the flow of intelligence information to critical partners. Obstacles reported by sector security specialists we interviewed include:

- The government does not have a good mechanism to quickly pass on classified threat information to the private sector. Classified threat information is provided to the few in industry who have the necessary security clearances, but there are thousands of small financial service providers who do not receive this information. Some mechanism is needed to get unclassified versions of threat information produced and distributed throughout the sector on a timely basis.
- Threat information is sometimes classified as “law-enforcement-sensitive,” which rarely is shared with the private sector.
- In some instances the government has a signed non-disclosure agreement with a company, restricting how government may share information received from that company with other private sector organizations and even other government entities.
- Information provided by the private sector for regulatory purposes may be highly constrained from sharing for security purposes. This is necessary to preserve the fidelity of the regulatory role and ensure an open flow of information between trusted partners in the regulatory regime. However, it impedes the flow of threat information across government partners and may prevent others in the private sector from learning about relevant attack or threat information from other companies in the sector.

4.2 Current and Emerging Models of Successful Information Sharing

Among the emerging models of successful information sharing between the sector and government, those interviewed noted especially work being done in the Government Information Sharing Network (GISF) program, continued close cooperation with the FBI, and the FSSCC all-hazards playbook for major disasters developed in coordination with the DHS National Infrastructure Coordinating Center (NICC).

New Information-Sharing Initiatives Are Being Pursued

There is a concerted effort to improve information sharing between the public and private sectors, driven primarily by the recognition on the part of both government and private industry that the cyber threat is beyond the capabilities of either to manage alone. Private sector security specialists point to two such information-sharing processes that hold promise for the future: the Defense Cyber Information Sharing Environment (DCISE) and the Government Information Sharing Framework (GISF).

According to one interviewee, information sharing has “leaped ahead” because of the DCISE, which is the focal point and clearing house for referrals of intrusion events on Defense Industrial Base (DIB) unclassified corporate networks. A collaborative operational information sharing environment among multiple partners, the DCISE produces threat information products for industry partners, who in turn provide notice of anomalies and share relevant information back through the partnership.[35]

The GISF was launched in 2010 as a collaborative effort between about a dozen financial firms and the FS-ISAC, which serves as the information sharing operational arm of the FSSCC, the DoD, and DHS. The GISF creates a trusted core of individuals, who using a subscriber agreement, gain access to direct threat and attack information at the "For Official Use Only" level.[36] Another recent development is collaboration between DHS and the FSSCC to develop protocols for sharing under specified conditions, as described in Figure BF-6.

Figure BF-6. FSSCC and DHS Collaboration: Developing Guidelines for Information Sharing

As a result of growing cyber challenges, innovative approaches are being taken by the sector and the Federal government to enhance the sharing of intelligence-derived information in order to better protect the nation's critical financial infrastructure. The NASDAQ hack (described in Figure BF-6) resulted in FSSCC and senior DHS officials agreeing to develop information sharing protocols under specific conditions. As Jane Carlin, FSSCC Chairperson, told Congress in April 2011: "The FSSCC and DHS have agreed to collaborate on developing guidelines for when information should be shared, especially information that is technical and contextual. FSSCC members believe that a more transparent decisionmaking process would accelerate the dissemination of information without interfering or undermining criminal and national security investigations. We also hope that these protocols will elevate the priority that government places on sharing information associated with protecting critical infrastructure. Also, by leveraging the security clearances that DHS and other government agencies have sponsored for members of the FSSCC, the government could consult with industry experts to better understand the systemic risk implications of the cyber events."

Close Cooperation with the FBI and the United States Secret Service (USSS)

The sector's relationship with the FBI and the USSS are excellent. Both groups are well respected, provide on-going trusted avenues for information sharing, and have good working relationships with bank security personnel. Supporting its role in anti-terrorism and criminal investigations, the FBI offers monthly briefings on a regular basis and special alerts on an as-needed basis. Many of the sector's security officers are former FBI agents, and this professional "alumni" association pays great dividends in terms of the quality and timeliness of sharing critical information. Similarly, counterfeiting and cyber crimes are handled by the USSS, with a mutually trusted flow of information. With respect to cyber crimes, for example, the USSS has developed and shared a wide range of valuable information based on extensive open-source work.

FSSCC All-Hazards Playbook Provides an Effective Approach

The FSSCC and FS-ISAC become involved with the cross-sector NICC during certain national emergencies, such as major hurricanes. During Hurricane Gustav in 2008, private sector representatives applied predictive analytics and used their contacts throughout the sector to identify locations where food, gasoline, building supplies, medicine, and other essentials could be purchased in impacted areas. This coordinated approach was also used during the 2010 earthquake disaster in Haiti. From this experience, the FSSCC has developed an all-hazards crisis event response playbook to coordinate the sector's response to large-scale incidents. The playbook provides a standard set of FSSCC operating processes and guidelines for assessing the situation, assembling the appropriate teams, and taking action to

[35] "DOD Deploys Effective Info Sharing to Address Cyber Vulnerabilities," Information Sharing Environment, October 13, 2010, http://www.ise.gov/news/dod-deploys-effective-info-sharing-address-cyber-vulnerabilities.

[36] *The Department of Homeland Cyber Security Mission: Promoting Innovation and Securing Critical Infrastructure, Before the Subcommittee on Cyber Security, Infrastructure Protection and Security Technologies of the Homeland Security Committee of the House of Representatives,* 112th Cong. (April 15, 2011) (written statement of Jane Carlin, Chairperson, Financial Services Sector Coordinating Council). http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Carlin_0.pdf.

coordinate the response. Specific scenarios considered include hurricanes and typhoons, pandemics, coordinated attacks, and public infrastructure failures. This was found to be an excellent approach for sector coordination that other sectors could adopt and tailor to their own needs.

4.3 Related Tools and Approaches for the Sharing of Intelligence Information

Because of the advanced maturity of many intelligence and information-sharing arrangements between the Banking and Finance Sector and the Federal Government, the case study participants were particularly interested in exploring with sector senior executives and subject matter experts various analytic models and tools that might have applicability across other sectors. This section describes some of these information sharing models.

Predictive Analytics

Predictive analytics, already proven to be a useful tool in law enforcement, could play an important role in the sector's cyber security, as shown in Figure BF-7. The Virginia State Fusion Center in Richmond reported that the center has used predictive analytics to predict identified threat vectors, such as likely locations for attempted theft of copper wire.

Figure BF-7. Banking & Finance Predictive Analytics Defined

Predictive analytics is a very specialized capability based on a variety of statistical techniques from modeling, data mining and game theory that analyze current and historical facts to make predictions about future events. Models capture relationships among many factors to allow assessment of risk or potential associated with a particular set of conditions, guiding decisionmaking for candidate transactions. Predictive analytics is used in actuarial science, financial services, insurance, retail, travel, healthcare, telecommunications, pharmaceuticals and other fields. One of the most well-known applications is credit scoring, which is used throughout financial services. Scoring models process a customer's credit history, loan application, customer data, etc., in order to rank-order individuals by their likelihood of making future credit payments on time.

Figure BF-8. Banking & Finance Signature Analyst for Infrastructure Protection

This method of predictive analytics, currently a pilot project within the DHS Science and Technology Directorate, brings together subject matter experts, tradecraft, and software to examine in detail past events to predict similar events occurring in precise locations in the future. It identifies hundreds of factors connected geographically (e.g., past events, infrastructure, demographics, transportation, economic and social-cultural conditions, elevation, satellite imagery), and applies advanced search algorithms to produce Probability Density Functions to find the highest probability for future events to occur.

Several companies specialize in the statistical approaches underlying predictive analytics. IBM's SPSS Text Analysis, for example, is used to discover connections and relationships in all types of unstructured data.[37] The Memphis Police Department has used IBM SPSS predictive analytics software to improve its overall operations and considerably reduce crime in its jurisdiction.[38]

Another example of the application of predictive analytics is the Signature Analyst for Infrastructure Protection program being developed jointly by the DHS Science and Technology Directorate (S&T) and GeoEye Analytics (see Figure BF-8). GeoEye specializes in geospatial predictive analytics, a statistical and

[37] According to Wikipedia, "SPSS is a computer program used for survey authoring and deployment (IBM SPSS Data Collection), data mining (IBM SPSS Modeler), text analytics, statistical analysis, and collaboration & deployment (batch & automated scoring services)."

[38] For IBM's description of its SPSS-based software, see "SPSS Modeler," IBM, http://www-01.ibm.com/software/analytics/spss/products/modeler/. For a list of success stories utilizing IBM SPSS predictive analytics, see "Success Stories," IBM, http://www-01.ibm.com/software/success/cssdb.nsf/softwareL2VW?OpenView&Count=30&RestrictToCategory=spss_SPSSModeler&cty=en_us.

analytical process that examines the geographic relationships between certain events and hundreds or even thousands of factors that influence where events have occurred in order to predict where similar events are likely to take place in the future. This tool has been effectively applied in war zones, such as Iraq, to predict where improvised explosive devices (IED) may be planted, and in areas of gang violence, such as Los Angeles, to predict where certain acts might occur.

Though these approaches hold promise for applicability to cyber attacks on financial institutions, they currently are beyond the financial and analytical capabilities of most mid- to small-sized financial institutions. Research must continue to find ways to leverage these tools across the sector and other critical infrastructure, while examining ways to make these capabilities more affordable and widely available. This area could likely benefit greatly from a coordinated Federal effort that leveraged economies of scale to deliver predictive-analytic capability to the tens of thousands of entities in the sector.

Capability Maturity Model

Information sharing among the government and private sectors across critical infrastructure industries is not uniform in maturity. One way to understand the role of maturity in the development of organizations is the Capability Maturity Model (CMM) developed by Carnegie Mellon University. Although there is no direct application of the model to intelligence-sharing partnerships, the stages of the model can be leveraged for such partnerships.[39] The five stages of CMM and definitions possibly applicable to intelligence-information sharing organizations include the following:

- **Stage 1: Initial** – first attempts at sharing of information between public and private sectors is usually based on personal trust relationships and past experience in dealing with each other in crises or other significant events
- **Stage 2: Repeatable** – building upon a few examples that work to make the exchange more frequent and across a broader range of issues
- **Stage 3: Defined** – organizing the processes in a more defined manner with roles and responsibilities communicated and expectations categorized
- **Stage 4: Managed** – managing the process with a goal to improve product and process quality
- **Stage 5: Optimizing** – continuous improvement through a feedback system and process change management

The original CMM has evolved through several versions, including CMMI (Capability Maturity Model Integration)[40] and more recently the Data Management Maturity (DMM) model, which focuses on processes. The DMM model is being applied to financial institutions to help audit data management components at the business-process level to improve enterprise management. Such audits assess multiple components within the categories of data governance and strategy, data operations, quality management, and data platforms, each of which can be measured in terms of the five stages of maturity described above. Because it can identity criteria and verify data integrated into systems, the DMM model may have applicability in intelligence and information-sharing systems as well.

[39] Mark C. Paulk, Charles V. Weber, and Mary B. Chrissis, "The Capability Maturity Model: A Summary," *Institute for Software Research*, paper 2 (Pittsburg, PA: Carnegie Mellon University, 1999), http://repository.cmu.edu/cgi/viewcontent.cgi?article=1013&context=isr&sei-redir=1#search=%22Mark%20C.%20Paulk%2C%20Charles%20V.%20Weber%2C%20Mary%20B.%20Chrissis%2C%20%E2%80%9CThe%20Capability%20Maturity%20Model%3A%20Summary%22.

[40] For an overview of CMMI, see "Overview," Software Engineering Institute, Carnegie Mellon University, http://www.sei.cmu.edu/cmmi/.

Wilhelm Model of Trusted Agents to Share Information

One model for the exchange of intelligence information between the public and private sectors builds on the work of Professor William Wilhelm of the University of Virginia and his colleagues who have described the critical role played by investment banks in sharing marketplace information between various investors and traders.[41] He argues that "financial markets cannot function effectively, if agents with valuable information are unable to sell it to those who require it…. Investment banks exist because they maintain an information marketplace that facilitates information-sensitive security transactions…. Investment banks use the threat of exclusion from a valuable long-term relationship to ensure that legally unenforceable agreements are honored."[42] In other words, investment banks use their position as a trusted agent to facilitate the exchange of sensitive information between parties that may not have fully developed long-term relationships or formal mechanisms for the exchange of this information.

This model should be closely examined for its potential application to the challenge of intelligence information sharing. By building on this example, public and private stakeholders in the sector could identify an entity to become the trusted information agent for the exchange of confidential critical-infrastructure-security information. It could provide the key elements for success if the DHS is to achieve its mission in the Federal Intelligence Community as the coordinator and champion of sharing with the private sector.

ChicagoFirst and Fusion Center Model

Regional organizations especially can have important relationships with local fusion centers. ChicagoFirst,[43] for example, has a strong relationship with the Chicago Fusion Center, where it can receive classified briefings in the center's secure facilities. The relationship also enables ChicagoFirst to become aware of law enforcement information that may impact the security of the organization's members in the Chicago area.

The ChicagoFirst relationship with its local fusion center is one way regional financial partnerships within RPC*first*, as well as other local financial institutions, might be able to gain access to sensitive information from government sources that might otherwise not be available. To be most effective, where such relationships can be developed, local fusion centers should make an effort to ensure that the classified and other sensitive information they receive is made suitable for local use, and thus provide more actionable analysis for local and regional financial institutions.

The NIAC is aware that many fusion centers have missions primarily focused on law enforcement intelligence and/or emergency management. However, in those centers which do or can incorporate capabilities to work with private-sector critical infrastructure, a close working relationship between local financial institutions and the fusion centers would greatly benefit their communities.

[41] Alan D. Morrison and William J. Wilhelm, Jr., "Investment Banking: Past, Present, and Future," *Journal of Applied Corporate Finance* 19, no. 1 (2007), http://gates.comm.virginia.edu/wjw9a/Papers/JACF%20Morrison%20Wilhelm%20Final%20version.pdf.

[42] Ibid., p. 10.

[43] Formed in 2003, ChicagoFIRST was the initial regional public/private partnership within the financial sector. Given its success, the approach has been replicated in more than a dozen regions of the country. See ChicagoFIRST homepage, 2011, https://www.chicagofirst.org/. There are 26 member institutions in ChicagoFirst and many Federal, State, regional, local, and private sector partners involved with the organization.

ISAC Model

As noted earlier, the FS-ISAC plays a pivotal role in the exchange of intelligence-derived information within the sector, as well as between the sector and various levels of government.

The ISACs were first articulated in Presidential Decision Directive-63 (PDD-63), signed May 22, 1998, which asked each critical infrastructure sector to establish sector-specific information-sharing organizations to share information about threats and vulnerabilities within the sector. In response, sectors established 16 ISACs to be trusted, sector-specific entities for full-time secure operations and alerting. ISACs establish their sector's specific information sharing/intelligence requirements for incidents, threats and vulnerabilities, and collect, analyze, and disseminate alerts and incident reports to their constituents, help governments to understand sector perspectives on security, and usually provide an electronic, trusted capability for its membership to exchange and share information on both cyber and physical threats. The ISACs are not uniformly active, however, nor do they all have the capabilities demonstrated by the FS-ISAC. The FS-ISAC is a model for the vital role these entities can play in information sharing.

5.0 Findings

Based on the data collected in this case study through interviews and open-source research, the Banking and Finance Sector case study members have ten findings.

Finding 1: Banking and Finance

Select nation-states and international organized-crime groups now pose advanced, persistent cyber threats that continue to threaten large financial institutions and have begun to target smaller companies with fewer security resources.

Private sector security directors we interviewed have seen a qualitative change in cyber attacks, which are becoming ever more sophisticated, targeted, smart, and innovative, using new attack vectors such as social media phishing attacks. Smaller companies often have limited security resources, affording them diminished levels of security protection compared to large financial institutions. Yet the inter-connected nature of the sector makes these smaller companies attractive targets as potential points of cyber access to larger organizations. A successful attack at one institution could cascade into others, making cyber security a shared threat among private-sector institutions.

Finding 2: Banking and Finance

Because of the interconnected nature of the sector, cyber security is not a competitive issue in the financial community. Rather, it is widely recognized that effective cyber information sharing requires a highly coordinated approach. Roles and responsibilities to implement this, however, are not yet clear among various government agencies and the private sector.

Conflicting missions among different government agencies with cyber security responsibilities can complicate coordination and slow the effective information sharing. Roles and responsibilities in the private sector become more complicated as financial institutions continue to rely heavily on private security companies, especially for cyber security.

Finding 3: Banking and Finance

The Banking and Finance Sector has experienced a "hamster-wheel" effect in cyber security: constantly increasing protection against the most recent attack mechanisms without having the necessary tools to anticipate the next one. Predictive capabilities that enable pre-emptive rather than

reactive security activity will become imperative as adversaries' cyber attack capabilities continue to evolve and grow.

With the shifting, ever-evolving nature of attacks, a purely reactive posture is doomed to failure. By leveraging new capabilities such as predictive analytics, public and private sector partners can get out ahead of the next style of attack.

Finding 4: Banking and Finance

Intelligence information sharing within the sector happens through strong and robust channels. This enables the sector to be less dependent upon personal relationships for critical information than other sectors.

The sector's history of regulation means that public and private sector participants have long-standing, trusted relationships and clear processes for interaction that are continually refined. For the most part, sector stakeholders involved in intelligence and other information sharing have well-developed roles and responsibilities in the information sharing process. The FS-ISAC is especially strong. Nonetheless, for certain kinds of time-sensitive intelligence, chief security officers in the sector still rely upon personal contacts to quickly acquire the information they need. Often, these individuals are former intelligence or law enforcement officials who have moved over to the private sector and can reach out to former colleagues who are still in government.

Finding 5: Banking and Finance

Private-sector stakeholders willingly share through trusted intelligence sharing relationships, which require a secure mechanism for information exchange, mutual benefit, and an established track record of confidentiality.

Trusted partnerships are built over time, as the participants learn each other's needs, capabilities, and commitment to honoring confidentiality. Each side of an information sharing partnership must see a benefit from the partnership's success, and be able to participate through secure, easily accessible, and user-friendly tools and processes.

Finding 6: Banking and Finance

The FSSCC is highly proactive in seeking ways to improve information sharing between the sector and the Federal Government, especially with the Department of the Treasury (the sector SSA), the USSS, and DHS. The sector's ongoing dialogue with the DHS Office of Infrastructure Protection to develop protocols for intelligence sharing during certain emergencies is working to fill gaps in intelligence sharing that still exist.

The FSSCC playbook for sector response to all-hazards crises, while not directly focused on information sharing between the public and private sectors, contains coordination information (such as contacts and procedures) that can expedite sector response to emergencies in ways that benefit both government and the private sector. By taking a proactive stance on this and other critical activities that facilitate coordination, the FSSCC is improving its access to critical information. Such relationship-building should be extended to the SSAs for the Communications and Information Technology Sectors, on which the Banking and Finance Sector is highly dependent.

Finding 7: Banking and Finance

There is evidence that many senior executives do not fully appreciate the risks their companies face from sophisticated, emerging cyber threats. Many companies do not have established points-of-contact at the executive level to interact with intelligence sharing organizations.

Senior executives require better knowledge about general cyber threats to the sector and specific threats to their organization. Sector security specialists reported that system operators often downplay threats or do not fully communicate the extent or impacts of known threats.

Finding 8: Banking and Finance

Physical threat information may be delayed in reaching a facility occupant because confusion exists over who is responsible for facility security: the owner in the Commercial Facilities Sector, or the tenant in the Banking and Finance Sector.

In reality, a threat to one is a threat to the other. The sectors need better coordination and need to provide clarity on roles to information sharing agencies to ensure that both entities receive the information they need to protect their respective assets.

Finding 9: Banking and Finance

Predictive analytics and other tools are needed to provide the sector with more proactive security measures, rather than post-event information that necessitates reactive measures.

Currently, intelligence-related information received from government is primarily post-event. The rapidly evolving nature of cyber attack modes makes predictive intelligence an *absolute necessity*, not merely a luxury.

Finding 10: Banking and Finance

Mission conflicts among government agencies must be resolved to prevent continuing harm following an infrastructure attack.

A delay in sharing known threat information during an ongoing law-enforcement investigation not only increases the vulnerability of business-sensitive data, but compromises the underlying foundation of trust built between the public and private sectors.

6.0 Conclusions

Banking and Finance Sector case study members have the following 10 high-priority conclusions that frame needed improvements in bi-directional sharing between the public and private sectors.

Conclusion 1: Banking and Finance

As cyber threats continue to grow in frequency and capability, government and private sector partners need to develop a more proactive stance on addressing threats, rather than the current reactive stance.

Stakeholders should focus on drawing in other government and private agencies and capabilities that can contribute to the overall cyber security of the sector. DHS has a vital role to play in this effort, because the Department has been assigned by Federal law and policies to be “the focal point for the security of cyberspace – including analysis, warning, information sharing, vulnerability reduction, mitigation efforts, and recovery efforts for public and private critical infrastructure and information systems.”[44]

[44] GAO Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, “Cyber Security: Continued Attention Needed to Protect Our Nation’s Critical Infrastructure,” GAO-11-865T, July 26, 2011, p. 2. http://www.gao.gov/new.items/d11865t.pdf.

Conclusion 2: Banking and Finance

The USSS should work closely with other appropriate cyber security agencies in the Federal Government and abroad, as well as with private-sector cyber-security experts, to devise systems and processes aimed at better protecting smaller companies from advanced, sophisticated cyber attack, which these companies do not have the tools or resources to defend against.

Conclusion 3: Banking and Finance

Federal agencies with cyber security responsibilities should work together to resolve mission conflicts that could enable continuing harm to the private sector following a discovered cyber or physical attack.

The health of critical sectors should be a high-priority along with other missions, such as law enforcement and intelligence collection.

Conclusion 4: Banking and Finance

This Banking and Finance Sector Case Study strongly endorses the four recommendations of the FSSCC as presented to Congress in testimony on April 15, 2011.[45]

These recommendations—detailed in the full testimony—are designed to improve the public-private partnership between the sector, DHS, and other government agencies. They include:

a. Protecting critical infrastructure through enhanced information sharing
b. Conducting more exercises and training
c. Investing in research and development (R&D)
d. Coordinating efforts internationally

Conclusion 5: Banking and Finance

DHS should take the lead in exploring new intelligence capabilities, such as predictive analytics, and helping the sector improve information sharing processes through tools such as the Data Management Maturity Model and the trusted information agent model.

To do so, DHS should focus on the following activities:

a. Continue its research and development on the applicability of predictive analytics to assist the sector and other critical infrastructures to protect against and mitigate the effects of future disruptive events.
b. Explore possible adaptations of Carnegie Mellon’s Data Management Maturity Model to critical infrastructure information-sharing processes to determine where these processes might be improved.
c. Examine how the trusted information agent model (developed by Professor William Wilhelm and others) might be applied to the information-sharing environment of critical infrastructure owners and operators and the Federal Government for the purposes of critical infrastructure protection and resilience.

[45] *The Department of Homeland Cyber-security Mission: Promoting Innovation and Securing Critical Infrastructure, Before the Subcommittee on Cyber Security, Infrastructure Protection and Security Technologies of the Homeland Security Committee of the House of Representatives,* 112th Cong. 9–10 (April 15, 2011) (written Statement of Jane Carlin), http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Carlin_0.pdf.

Conclusion 6: Banking and Finance

The FSSCC should collaborate with the Financial and Banking Information Infrastructure Committee (FBIIC), FS-ISAC, DHS, and other public and private security partners to institute executive-level educational programs that increase understanding of emerging cyber threats to the financial services industry.

Each company should identify executive-level points of contact to interface with information-sharing agencies on classified and unclassified threat information to ensure that threats are well understood and cyber security is given the appropriate priority within all financial institutions.

Conclusion 7: Banking and Finance

RPC*first* member organizations should engage their local fusion centers to determine if a useful information-exchange partnership can be developed.

Fusion centers enable the private sector greater access to wider ranges of threat information at a regional level. Where appropriate, local fusion centers should also proactively reach out to local financial institutions with the same purpose in mind.

Conclusion 8: Banking and Finance

ODNI should guide the Federal Intelligence Community members to create unclassified versions of intelligence documents that can be rapidly disseminated to critical infrastructure sectors for their own protection and resilience efforts.

Useful threat information—which may not be classified in and of itself—may be locked inside classified intelligence products that can only be accessed by the few private sector members with clearances. Unclassified versions, distributed more widely, can help the private sector take proactive security steps.

Conclusion 9: Banking and Finance

The USSS and other law enforcement agencies at all levels of government should add a question to their investigative reports that identifies any impacts on critical infrastructure that may result from or be part of the incident being investigated.

The law enforcement community should devise a mechanism allowing this impact information to be forwarded to (potentially) affected infrastructure owners and operators in a timely fashion.

Conclusion 10: Banking and Finance

Other critical infrastructure sectors should consider the FSSCC all-hazards crisis event response playbook as a model for how to coordinate information exchange during large-scale emergencies.

This provides a highly useful model to assure effective identification, understanding and integration of private-sector capabilities, and the leveraging of these capabilities for a true national response to emergencies.

Appendix C. Case Study: Chemical Sector

TABLE OF CONTENTS

1.0 Introduction

Overall, the Chemical Sector is well organized for security and companies have collaborated effectively through industry associations and trade groups for many years. Most major chemical companies are knowledgeable, engaged, and cooperative on security matters, due in part to a culture of working together on noncompetitive issues. These major companies generally have good access to government threat and vulnerability information for both physical and cyber assets. By contrast, smaller companies are often less engaged in homeland security issues and may not be familiar with many of the information-sharing mechanisms that are available.

The Chemical Sector, working through the Critical Infrastructure Partnership Advisory Council (CIPAC) partnership model, has noticed clear improvements in information sharing over the past five years. Information-sharing mechanisms have matured and a strong relationship with the U.S. Department of Homeland Security (DHS) Chemical Sector-Specific Agency (SSA) has improved the quality and relevance of information provided to the sector. Yet despite these improvements, owners and operators are frustrated by a lack of understanding within government of their security information needs, insufficient coordination within and among government agencies, and deficiencies in information systems that sometimes fail to get the right information to the right people in a timely manner. The Chemical Sector believes that more needs to be done to streamline and simplify sharing mechanisms; gather and disseminate threat data that is useful to the sector in bolstering security practices; better clarify authority and accountability among Federal agencies responsible for sharing threat information; minimize confusing and duplicative information streams and reporting requirements; and create formal and sustainable channels for partnership.

2.0 Sector Profile

Several hundred thousand facilities in the United States use, manufacture, store, transport, or deliver chemicals, as part of an industry that converts raw materials into more than 70,000 diverse products and brings in $637 billion in annual revenue. The Chemical Sector handles basic chemicals, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer products through a nationwide and global network of customers, distributors, and suppliers and is one of the major exporters in the U.S. economy. Facilities typically fall into one of four areas:

1. **Manufacturing Plants**—Receive, store, and process raw chemical ingredients to convert them into intermediate and end products.
2. **Transport Systems**—Both domestically and internationally transport chemical products through terminals, rail, highway, waterways, air, and pipeline.
3. **Warehousing and Storage Systems**—Store and repackage high volumes of chemicals, enabling the sector to build an inventory and maintain a steady flow of raw materials and products to maintain business continuity with customers.
4. **Chemical End Users**—Represent an array of chemical consumers including the food services, agriculture, healthcare, mining, science and technology, and education industries.

The sector employs more than 1 million people at a wide range of facilities from multi-billion-dollar corporations to small and specialized chemical manufacturers. While DHS estimates that 50,000 or more facilities may possess chemicals of interest, only 4,600 facilities are covered by the Chemical Facilities Anti-Terrorism Standards (CFATS), which regulate the highest-risk chemical facilities. Larger corporations may handle greater volumes of hazardous materials and have a higher risk profile. Because of their size, they often possess greater resources and manpower to address their risks. However, smaller corporations with limited security budgets may also manufacture or handle hazardous materials.

Operating and Security Characteristics

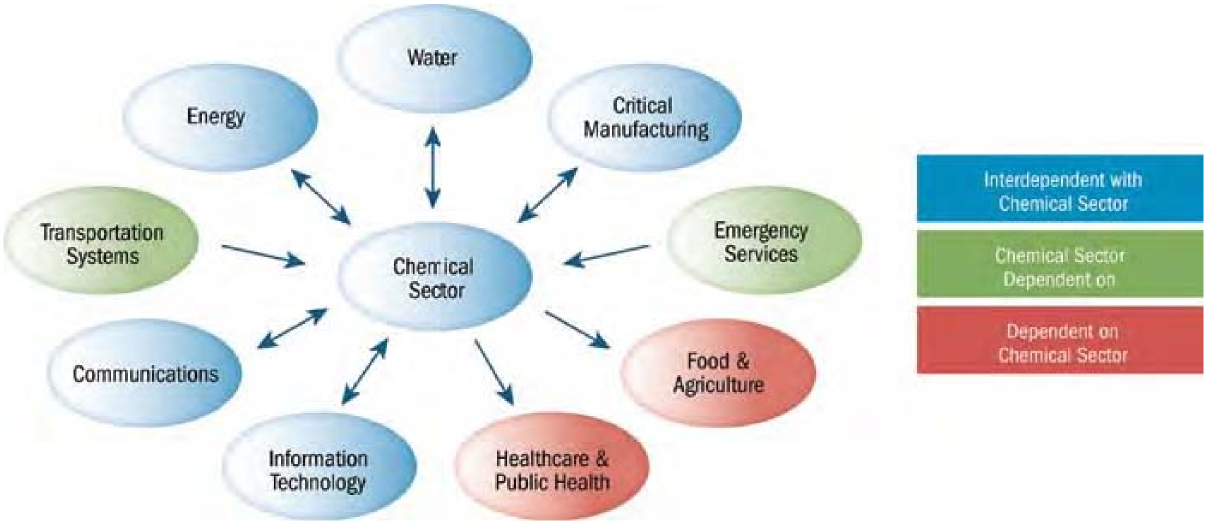
Unlike some critical infrastructure sectors, chemical manufacturing and storage plants are typically guarded and secured facilities with limited public access. Extensive safety and security measures include deterrents such as concrete walls, fences, closed-circuit television, electronic access control, perimeter surveillance and security guards (often contracted) that provide around-the-clock protection. Many facilities are located in remote and rural locations and depend upon a nationwide and global transportation network connecting suppliers, facilities, and end users.

Modern chemical manufacturing and transport integrate advanced cyber technology through a series of process control and safety systems, creating a close integration of physical and cyber security. Cyber systems operate manufacturing processes; track inventory, storage, and transport of chemicals; operate perimeter security and access control systems; and store customer and personnel information. Companies are increasingly likely to include an information technology security representative on their vulnerability assessment, crisis management, or emergency response team.

Historically, crime and natural disasters have posed the largest security and incident-recovery concerns for the sector. Chemical inventories and storage facilities enable the sector to withstand short-term service disruptions. The consequences of the misuse, release, or destruction of hazardous chemicals, however, make the security of the Chemical Sector among the most critical to public and environmental health and safety.

Interdependencies

In addition to a high dependency on the Transportation and the Emergency Services Sectors (particularly by smaller facilities for the latter), the Chemical Sector relies on and provides necessary services to several other critical sectors, including Energy, Water, Information Technology, Communications, Healthcare and Public Health, and Agriculture and Food.



History of Regulation

The Chemical Sector has a lengthy history of proactive and voluntary implementation of security measures and of successful compliance with legislation and regulations addressing health, safety, accident prevention, emergency response, and the environment. More recent legislation has focused specifically on chemical security, namely the Chemical Facility Anti-Terrorism Standards (CFATS), enacted in 2007, and the Maritime Transportation Security Act of 2002 (MTSA).

The Chemical Sector is subject to security-related regulations from multiple government agencies. Under CFATS, DHS collects facility data and assigns those facilities that are deemed to be high-risk to one of four tiers based on the public health and safety risk and mission critical aspects of a facility's products. High-risk facilities are required to perform a detailed consequence analysis and vulnerability assessment on those physical and cyber assets associated with each chemical of interest. Under MTSA, DHS can require chemical facilities adjacent to navigable waters or that interface with high-risk vessels to assess the likely consequences of an attack and conduct a vulnerability assessment of their facility. They can also require Transportation Worker Identification Credentials (TWICs)—tamper-resistant biometric credentials for workers accessing secure areas of MTSA-regulated ports, vessels, and facilities. Under the Transportation Security Administration and Department of Transportation there are regulations for rail and highway transportation of hazardous materials.

A key element of regulatory requirements is the prevention of and preparation for an emergency. The development of emergency response plans is a core process in the Chemical Sector and is also often required as part of CFATS, MTSA, the Environmental Protection Agency's Risk Management Program, the Resource Conservation and Recovery Act, and Occupational Safety and Health Administration (OSHA) regulations.

3.0 Assessment of the Current Information Sharing Framework and Processes

Security is widely viewed within the Chemical Sector as a collective responsibility, because a security breach at any U.S. chemical facility could affect the reputation and security posture of the entire sector. The chemical industry has a long history of cooperation on noncompetitive issues such as safety, security, and the environment. Collaboration on security is typically organized through chemical industry associations, such as the American Chemistry Council (ACC), the Society of Chemical Manufacturers and Affiliates (SOCMA), the Institute of Makers of Explosives (IME), the National Association of Chemical Distributors (NACD), and the International Liquid Terminals Association (ILTA), to name a few. Companies also coordinate at the local level through State chemical associations, mutual aid groups, and local emergency planning committees (LEPCs). Having an established culture and mechanisms to collaborate has allowed the industry to become proactive on chemical security issues. Industry executives and security directors with whom we spoke expressed a strong sense of duty to protect the public and a high degree of trust and respect among themselves.

To examine information sharing in this sector, a team of industry leaders interviewed about 30 individuals with information-sharing and security responsibilities across the sector, through one-on-one interviews and multiple roundtable discussions held with industry organizations such as the Society of Chemical Manufacturers and Affiliates (SOCMA), the Institute of Makers of Explosives (IME), and the Chemical Sector Coordinating Council.

Security Responsibilities and Information Needs

Security responsibilities and resources within chemical companies vary based on the size and structure of the enterprise. Large, global companies often manage security by geographic regions with centralized coordination. We interviewed many directors of corporate security, typically vice presidents, who are responsible for security (and often safety) across the global enterprise or for the North American region. These companies typically have full-time operations centers and dedicated staff who manage security operations and analyze threat and intelligence information, although some functions may be contracted out. Facility security managers have varying degrees of responsibility and autonomy depending on the particular chemical company.

At smaller companies, security managers typically wear multiple hats with additional responsibilities that may include compliance, safety, and certain operational duties. As security may likely be only 20%–25% of their job responsibilities, these security managers find little value in general threat information not specific to their operations and often do not have time to seek it out through online repositories. Though many engage through their industry associations, some do not and may remain isolated from information-sharing efforts. Smaller companies continue to have the fewest information sharing connections with government. However, because of their size, many companies consider themselves to be low-threat facilities regardless of whether they are regulated under CFATS.

Chemical Sector security managers are responsible for protecting company assets and systems; ensuring the safety of employees, contractors, vendors, and customers; and planning and preparing for chemical emergency response. Accordingly, they require specific and timely information regarding immediate threats to both chemicals at their facilities and in transit. They use this information to implement protective countermeasures and mitigation strategies. Their security teams also oversee the screening, detection, and prevention of all hazards, which requires both increased situational awareness and proactive information on ongoing threats that can help a security team bolster and tailor their preventive response. Many companies operate globally and need additional information on threats to foreign facilities and global transportation networks. Companies also need timely information on cyber risks, especially potential vulnerabilities to industrial control systems, and appropriate mitigation measures.

Cyber Security Information Needs in the Chemical Sector

Physical and cyber security functions are frequently managed separately, although some companies are working to integrate the two. Cyber security responsibilities are often further divided between the security of information technology (IT) and business networks on the one hand and the security of industrial control systems on the other. Industrial control and process safety systems that automate critical physical processes are large, complex, and often proprietary systems that require different cyber security measures than the IT systems that operate inventory and customer billing systems. As a result, specific guidance on monitoring and mitigation measures that companies can tailor to their systems is far more valuable than general cyber threat and vulnerability information, especially for smaller organizations.

Interviewees reported that the community of cyber security professionals in the Chemical Sector numbers fewer than 100 individuals worldwide and often shares vulnerability and incident information only in small, informal circles where continuity of individuals and personal relationships have built significant trust. Smaller companies, which do not have dedicated cyber security specialists or that rely primarily on system vendors for security, may be left out of these communities. Owners and operators often hesitate to disclose specific vulnerability or incident information with the cyber community or the government, fearing unknown legal liabilities or risks if the information is leaked. The threat of zero-day attacks—those that exploit vulnerabilities with no known mitigations—prevent companies from widely sharing vulnerabilities they find in their systems. Timely threat and vulnerability information, accompanied by specific identification and mitigation guidance, is needed to halt the spread of fast-moving or targeted cyber attacks.

Chemical Sector Information Sharing Relationships

The Chemical Sector was an early adopter of the public-private partnership for critical infrastructure protection through the Critical Infrastructure Partnership Advisory Council (CIPAC). CIPAC creates the legal framework to enable the two-way flow of information between the government and critical infrastructure owners and operators in a protected environment that encourages sharing. This framework is particularly important for the Chemical Sector because it maintains two distinct relationships with DHS: voluntary (through the Chemical Sector-Specific Agency [SSA]) and regulatory (through CFATS).

The public-private partnership provides an important platform for information sharing. The Sector Coordinating Council (SCC), which includes representatives of major chemical companies and industry associations, plays a prominent role in representing the chemical industry's security information requirements and in providing informational needs to the government. The SCC maintains a very close and supportive relationship with the DHS Chemical SSA, even though personnel have changed over the years. The Council works with members of the Chemical Sector to leverage DHS information sharing tools and processes, including the Homeland Security Information Network – Critical Sectors (HSIN-CS) and suspicious activity reporting.

Private companies, working through the SCC and its industry associations, continue to build an active partnership with other government components as well, such as the Department of Justice's Joint Terrorism Task Forces (JTTF), the National Interagency Coordination Center (NICC), and other elements of the intelligence community. Security directors for large chemical companies may maintain personal relationships with individuals within intelligence agencies, especially if they were previously employed at one of those agencies.

Key Information Sources and Mechanisms

The chemical security managers we interviewed rarely rely on a single mechanism for receiving information on threats, intelligence, and security trends. Companies use a wide variety of Federal and private mechanisms to collect data and intelligence about security risks. The most valuable and common resource is personal relationships and networks that are used to gather information, validate reports, or to gain additional context on official reports, helping chemical companies translate threats into practical security measures. Information sources and mechanisms that were mentioned in our interviews include HSIN-CS, the DHS Chemical SSA, industry associations, the Executive Notification System, the U.S. Coast Guard Home Port, DHS Protective Security Advisors (PSAs), the FBI and InfraGard, the Joint Terrorism Task Forces, the Domestic Security Alliance Council, private security companies, and select fusion centers. For information on international security risks, companies access information from the Overseas Security Advisory Council, the International Security Management Associations, private companies (such as iJet and SOS International), and foreign intelligence agencies. For cyber-related events, companies rely on the U.S. Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), system vendors, national laboratories, the Industrial Control Systems Joint Working Group (ICSJWG), the DHS National Cyber Security Division, and personal networks.

Security managers noted the importance of having alerts and threat information "pushed out" to them through emails and other means. Chemical security personnel may be traveling or mobile within a facility and getting information pushed to them is a key advantage. For alerts and immediate threats, timeliness is critical. News media and private security companies, which may report partial or unverified information, are often faster at getting information to chemical security managers than government sources. Some chemical security managers noted that there is often too much redundant information that can overwhelm them during a crisis. It was also noted that redundant information moved through multiple channels can also push certain information to the wrong company contact and cause unnecessary alarm and unintended consequences.

One interviewee characterized three types of classified government threat and intelligence information that affect critical infrastructures. There is “credible and imminent” threat information directed at specific facilities, for which there are numerous effective mechanisms for quickly notifying companies that are at risk. A second type of information covers general terrorist or criminal trends that are often communicated to the private sector through semi-annual classified threat briefings. The third type of information, which is not often shared with companies, includes partly credible, fragmented intelligence that government intelligence analysts are actively working on to “connect the dots” before it is shared with the private sector. This last type of intelligence represents a potentially valuable source of information for the private sector, if it can be presented and communicated effectively.

Classified information is typically disseminated to chemical companies through twice-yearly classified threat briefings. There are currently 132 chemical industry representatives who hold security clearances and roughly 30–35 attend classified briefings on a regular basis. The briefings are designed specifically for the chemical industry and cover emerging trends. The briefings are presented by analysts from DHS Intelligence and Analysis (I&A), the FBI, and other agencies. Because the briefings must be held in a secure facility, most briefings are conducted in Washington, DC. This requires chemical company representatives to travel and thereby limits the accessibility and frequency of classified briefings.

The DHS Chemical SSA also shares non-classified information with the chemical industry through a monthly suspicious-activity teleconference call organized through HSIN-CS, which several security managers found important to maintaining their situational awareness.

4.0 Effectiveness of Information Sharing in the Chemical Sector

According to most chemical security managers we interviewed, significant improvements have been made in public-private information sharing since 2006, when the NIAC first studied public-private intelligence coordination. A typical refrain was, “More needs to be done, but it is a lot better than it was.”

Despite some deficiencies, information sharing mechanisms such as HSIN-CS and US-CERT have matured to become more respected conduits of information from the Federal Government and its intelligence agencies, which are beginning to view the private sector as a legitimate customer of threat information and a partner in security. Many security managers we interviewed said HSIN was a primary source of threat information they could use—a “premier tool for information gathering”—while others found it to be frustrating to access and behind the curve on real-time threat information—“like reading last week’s weather report.” Many are unaware of its capabilities and personalized settings, while many smaller companies are not aware of its existence. Interviews with five security managers from smaller chemical companies revealed that not one had heard of or used HSIN. A common criticism of HSIN and similar “pull” mechanisms is that chemical security managers must use critical time mining them for relevant threat information.

Chemical companies have leveraged their relationship with the Chemical SSA to get better intelligence (for example, on criminal activity along the U.S.-Mexican border), and to help improve the quality of the sector's twice-yearly classified briefings. Companies requested more detailed, relevant information in feedback to the SSA, which continues to educate intelligence analysts (from DHS, the FBI, and other agencies) on chemical security information needs in order to deliver more valuable briefings.

During regional emergencies and natural disasters, unclassified information sharing between the Federal Government and private sector (through teleconferences and briefings) is frequent and effective, helping businesses to restore critical services more quickly. But the government lacks a system to swiftly distribute urgent threat alerts and information to the right people as a situation unfolds. Timeliness is critical for alerts and immediate threats, and security managers noted this is a time when alerts should be "pushed out" to them. But one interviewee indicated that during a quick-moving incident, he believed he would likely get information from a national news organization faster than from the government or many of the Chemical Sector organizations, though the information may be partial or unverified. Perhaps the most persistent and fundamental barrier to effective information sharing with the Chemical Sector, though, is the lack of private-sector experience and subject matter expertise among intelligence collectors and analysts that limits understanding of Chemical Sector security needs. This was a key finding of the 2006 NIAC study and it continues to be an area for improvement. Though the detail and relevance of classified briefings have improved since 2006, a limited understanding of the sector means that intelligence analysts do not always gather or present information with private-sector needs in mind. This disconnect is best characterized by a description of one classified briefing concerning a bombing in Saudi Arabia in which the Chemical Sector security managers present wanted tactical information such as the size of the vehicle, how the attack occurred, whether the gate was open or closed, and whether the uniforms were stolen or made, but the intelligence analysts conducting the briefing were providing information about the go code, funding, and the hierarchy of the terrorist organization.

Suspicious-activity reporting from chemical companies to the Federal Government has become a common practice that contributes to greater security and awareness. According to one government official, roughly 80% of all thwarted attacks are in response to a suspicious activity report (SAR) at the local level. The vigilance of chemical company employees to report suspicious activities has been reported in several national news stories (see Figure C-1 for an in-depth example) and can help analysts connect the dots among multiple related incidents. In one case, a group of suspicious individuals had entered two non-chemical establishments in a Florida town seeking information on their operations. An SAR from each company enabled an analyst at the local fusion center to make the connection between the two and follow up with each. But this isn't yet happening on a consistent basis at the national or regional level. Stovepiping among fusion centers at the local level and intelligence collectors at the national level has prevented analysts from looking across regions and sectors to connect the dots on similar suspicious activity reports or other threat information—especially because SARs do not end up in a universal data set, and intelligence analysts are rarely assigned to examine threats across a sector.

Figure C-1. Chemical Company Helped Thwart Texas Terror Plot

On February 1, 2011, the chemical company Carolina Biological Supply of Burlington, N.C. helped thwart plans of a college student who planned to hide bomb materials inside dolls and baby carriages to blow up dams, nuclear plants, or the Dallas home of former President George W. Bush. Khalid Ali-M Aldawsari, a 20-year-old student from Saudi Arabia who studied chemical engineering in Texas, made an online purchase of $435 worth of phenol, a chemical used in college-level organic chemistry classes and common household disinfectants, but also a precursor to the explosive trinitrophenol, also known as TNP. One day after shipping the product, the company suspected that the order was suspicious and notified the FBI.

Separately, Con-way Freight, the shipping company, notified local police and the FBI about similar suspicions because it appeared the order wasn't intended for commercial use. Federal agents traced Aldawsari's other online purchases, discovered extremist posts he had made on the Internet, and secretly searched his off-campus apartment, computer, and e-mail accounts and read his diary.

"We couldn't see the whole picture. We didn't know the whole scope," said Keith Barker, Carolina Biological Supply's manager of product safety and compliance. "It's pleasing that we apparently helped thwart the plot."

TNP, the chemical explosive that Aldawsari was suspected of trying to make, has about the same destructive power as TNT. FBI bomb experts said the amounts in the Aldawsari case would have yielded almost 15 pounds of explosive. That's about the same amount used per bomb in the London subway attacks that killed scores of people in July 2005. Aldawsari is also suspected of plotting to place car bombs in different places during rush hour in New York City and remotely detonating them.

This example underscores the important role that private-sector companies have in exposing potential threats and the willingness of chemical and shipping companies to share suspicious-activity information with the Federal Government and local law enforcement.

Based on a news report by Adam Goldman and Betsy Blaney, *The News & Record*, Greensboro, NC.

One frequent comment from Chemical Sector security managers was that SARs they provide to the government rarely elicit feedback to indicate whether an investigation was initiated or where it led. Just knowing that a suspicious incident was insignificant is helpful to private-sector security managers (see Figure C-2 for an in-depth example). A lack of feedback discourages continued sharing and reduces the effectiveness of "neighborhood watch" practices, when employees are frequently placed on high alert, because there is no follow-up to indicate that the suspicious activity concerned has been addressed. It also reinforces a continued reliance on personal contacts in the government, who companies frequently contact when feedback is lacking or to get more context on information the government has shared. One interviewee said his company would be "out in left field" without contacts.

Another frequent frustration in the Chemical Sector is the lack of coordination among government agencies, even within agencies, that leads to multiple and redundant channels of information to chemical companies, as well as redundant and uncoordinated requests for information. While regulatory relationships keep companies in close contact with multiple Federal agencies (e.g., DHS, TSA, U.S. Coast Guard), they face multiple reporting requirements that force security managers to spend more time on the phone reporting an incident than actually addressing it. The lack of internal information sharing among Federal departments and intelligence agencies can slow response and place responsibility on the private sector to ensure information arrives in the right hands. Although Chemical Sector managers understand the challenges that the government faces in collecting, analyzing, tailoring, and disseminating information for multiple sectors, they feel more leadership is needed to achieve better integration of Federal resources and more streamlined processes.

Figure C-2. Malicious Sabotage of Chemical Delivery Truck

Two days before Christmas, a delivery-truck driver for an industrial-gas supplier pulled his cryogenic trailer into a commercial truck stop for a layover, parked at the back of the facility (out of sight of the main road), and checked into the adjacent motel. At 6:30 the next morning, he received a call from the company dispatch that there was a problem with the truck. Once outside, he found the local fire department and police responding to a liquid oxygen cloud coming from the truck. After the driver stopped the leak and inspected the truck, it became clear that someone had maliciously opened two valves that released liquid oxygen in a very specific and controlled way. After the release was contained and the first responders left, the driver discovered that a diesel fuel line underneath the truck had been purposely cut, causing diesel fuel to spill onto the ground. In all, about 15,000 gallons of liquid oxygen and 3 gallons of diesel had been spilled. The combination of the liquid oxygen and diesel could have caused a serious fire had there been an ignition source. The driver contacted police about the cut diesel line and they updated their report. The company was not contacted again by local police concerning any investigation

The company's corporate security team also reported the incident to the DHS NICC through their online portal. Although the company typically hears back from the NICC within 24 hours of making such reports, they were not contacted for this incident. After several days the company again attempted to reach a local investigator but was unsuccessful. Having gotten no response from the local police or the NICC, the company then contacted the FBI office closest to the company headquarters and the DHS PSA in the region where the incident occurred, and provided them with the same information. Following these two contacts, the company received a call from the fusion center for additional follow up. During this conversation, the company learned that the report that the fusion center received from the NICC was inaccurate and incomplete, merely indicating that a liquid oxygen leak had occurred.

Once the company corrected the facts, the JTTF launched an investigation. When it was determined that the incident was not an act of terrorism, the company did not hear back from the government.

This example highlights multiple breakdowns in information sharing. The local police did not appear to treat this incident as a serious crime. The NICC may not have understood the significance of the incident or may have misinterpreted the facts. Although the company followed the government procedures for reporting incidents, it had to continue to insist that the incident be investigated both at the local and Federal levels. The feedback loop to the company on the outcome of the investigation was not completed.

5.0 Findings

Based on the data collected in this case study through original interviews and open-source research, the Chemical Sector Case Study members believe the following nine findings best summarize the status of intelligence information sharing in their sector.

Finding 1: Chemical

Personal relationships continue to be important for Chemical Sector information sharing.

- Personal relationships that Chemical Sector security managers maintain with Federal Government contacts, law enforcement, and their industry peers are highly important for gathering and interpreting threat and intelligence information.
- Locally, relationships with the Protective Security Advisors are varied, but where strong relationships exist they provide a useful source of information for security managers. Law enforcement relationships are deemed important for reporting suspicious activities of a local nature.
- Most security directors of major chemical companies are well connected with each other through the Sector Coordinating Council, industry associations, and personal relationships. They leverage their relationships to share information on incidents, emerging security issues, and protective measures.

Finding 2: Chemical

The Chemical Sector has an excellent and productive relationship with the Chemical Sector-Specific Agency and views it as a key, valued information-sharing asset for the industry.

- The strong relationship between chemical security managers and the DHS Chemical SSA is valuable in gaining access to and analyzing intelligence from Federal Government sources.
- The Chemical SSA plays a proactive role in helping chemical companies obtain the intelligence information they need and serving as an advocate of industry concerns and needs within the Federal Government.
- Engagement with some smaller companies is often facilitated through local industry councils and associations.

Finding 3: Chemical

Government intelligence provided to the Chemical Sector often does not meet the needs of chemical companies.

- There is a lack of understanding across government of Chemical Sector operations and their intelligence needs, due in part to a lack of chemical industry knowledge and subject matter expertise.
- Intelligence reports are designed to meet the needs of State and local government officials, not chemical owners, resulting in little practical or actionable information that can be translated into facility security measures.
- While DHS requests that industry share information on incidents to enable government analysts to "connect the dots," this is not reciprocated, inhibiting industry security analysts from participating in making critical connections.
- There appears to be a large amount of potentially valuable intelligence information that lies between the "credible/actionable" information and "general trends" information, which could be very valuable for knowledgeable Chemical Sector security managers who could aid the government in their analysis.

Finding 4: Chemical

Classified briefings were generally viewed as not very helpful, although they have improved.

- Chemical Sector security directors indicated that most of the information included in classified briefings can be found in mainstream media reports.
- Government briefers and analysts often have a poor understanding of the type of information that Chemical Sector security managers need, such as specific tactics and attack methods that would enable companies to develop practical countermeasures at their facilities.
- Classified briefings have improved as a result of feedback given to the SSA, which worked with DHS analysts to develop more tailored briefings and with the chemical industry to identify specific needs.

Finding 5: Chemical

The value of HSIN-CS as an information sharing tool within the Chemical Sector is mixed.

- Many sector representatives found HSIN-CS to be a useful source of reliable information that is used throughout the sector, but it could be greatly improved.

- The biggest criticism is that it is a “pull” system rather than a “push” system. Users must log in and extract information rather than having alerts pushed out to them through an e-mail or other means.
- Ease of access has been an issue because, when not used regularly, it is hard to navigate and passwords are forgotten. Also, security managers are frequently travelling. Others noted that the information is not real-time and typically presented at too high a level, making it of limited use during a crisis.

Finding 6: Chemical

Small companies often do not have good access to threat and intelligence information.

- Security managers in small companies frequently wear several hats and have limited resources to engage at the national level.
- They are rarely contacted by DHS, although many companies recognize they are low-priority targets due to their size and location.
- Some companies rely on their industry association to provide them with threat and intelligence information, yet many small or independent companies covered by CFATS are not members of industry associations.
- Few of the smaller companies we spoke with had an active relationship with the SSA.

Finding 7: Chemical

Cyber information-sharing norms are quite different from physical-security norms.

- Cyber security information on industrial control systems is shared within a small industrial community that requires a high degree of knowledge, confidentiality, and trust (perhaps 100 true experts worldwide).
- The cyber security community uses different information sources such as ICS-CERT and personal networks of technical colleagues.
- Vulnerability disclosure is a highly-sensitive area due to company exposure and the potential for a zero-day vulnerability.

Finding 8: Chemical

Chemical companies are readily willing to share incident information with the government, although most are frustrated by the lack of government follow-up and feedback.

- Every company representative with whom we spoke indicated a willingness and a sense of responsibility to share information about suspicious activity and incidents with the government.
- Government follow-up and feedback to the reporting chemical company is poor and acts as a disincentive to further share information with the government.
- In several information sharing situations a company’s name was made public; even if the company name is not released, DHS frequently identifies the company location, which de facto identifies the company.
- Sharing of cyber incidents with the government is much more sensitive because a company may not wish to expose a security breach.

Finding 9: Chemical

Fusion centers do not appear to play a big role in information sharing within the Chemical Sector.

- Many chemical companies do not rely on fusion centers for threat and intelligence information, and most have had little or no contact with fusion centers.
- Fusion centers are viewed as highly variable, with some centers reaching out to the local chemical companies and providing useful information and others not engaging with chemical companies at all.
- Many fusion centers focus on the law enforcement community and related activities. Some do not appear to understand, value, or know how to partner with the chemical companies.

6.0 Conclusions

Chemical Case Study members believe the following nine conclusions are of the highest priority for information sharing in the sector.

Establish Direct, Efficient Information-Sharing Processes

Conclusion 1: Chemical

Create a formal network of chief security officers and site security managers to facilitate public-private information sharing by designating a security point-of-contact within every high-risk and/or regulated chemical company.

- Build upon the network of contacts required by existing regulations and expand to encourage all companies to designate a national-level contact and regional/site-level contacts as appropriate.
- The DHS Chemical Sector SSA could lead the effort by working through regulatory agencies, industry associations, and the SCC, and share contacts with the fusion centers or other selected organizations.
- Direct the government to set up a parallel structure, in which each intelligence and regulatory agency designates a chemical industry POC to work with this network.

Conclusion 2: Chemical

Create an ODNI/DHS core of 3–4 cross-agency government analysts whose mission is to create and disseminate tailored and practical intelligence to the sector and otherwise respond to sector information needs.

- Analysts will operate at the national level but push out chemical-specific information to the fusion centers or other appropriate organizations and through the sector's network of security officers.
- Analysts' primary performance objectives will be to disseminate actionable information (not create intelligence products) and close the feedback loop when the sector provides information to the government.
- Analysts will meet with a small number of chemical industry SMEs twice yearly to garner feedback on sector information needs.

Conclusion 3: Chemical

DHS should work with the U.S. Intelligence Community to use classified information to develop timely, actionable intelligence products below the tear line for wide dissemination.

- As part of every classified briefing, require agencies to produce a corresponding unclassified version that can inform site personnel and enable companies to better prepare and respond.
- Use tools such as checklists (especially for cyber threats) that companies can use to determine how the information applies to their operations and what actions they should take.

Conclusion 4: Chemical

DHS should take the lead to Integrate information dissemination and eliminate conflicting reporting requirements among regulatory and intelligence agencies (e.g., TSA, USCG, DOT, DHS, FBI, CIA).

- Minimize unnecessary multiple or conflicting communications by harmonizing information into one message stream, potentially delivered through the Federal Chemical Sector analysts, the fusion centers, or other appropriate organizations.
- Create a single clear pathway for the private sector to report suspicious activity and incidents to all necessary agencies.

Better Engage Smaller Companies in the Information Sharing Process

Conclusion 5: Chemical

With DHS support, launch a coordinated outreach effort by Federal and State governments to take information “the last mile” to the local and site level and better engage smaller companies.

- Create active communities at the regional/local level by charging fusion centers or other regional/State organizations to proactively seek participation from both regulated and non-regulated companies and hold regular information-sharing meetings. The U.S. Coast Guard Area Maritime Security Committees can serve as a successful model.
- Use advertisements, PSAs, LEPCs, and State homeland security organizations to reach out to small companies and educate them on the basics of the Chemical Sector information-sharing process (such as HSIN, fusion centers, US-CERT).
- Encourage routine interaction between smaller companies and local law enforcement and State authorities in security planning for regulated facilities.

Conclusion 6: Chemical

Ensure the continued success of industry engagement through associations by not excluding registered lobbyists from participating in Chemical Sector CIPAC discussions.

- Review the unintended impact of the proposed policy on Chemical Sector information sharing. In the Chemical Sector, key knowledgeable participants and owner/operators are registered lobbyists because of the role they play in industry associations and, under the new rules, would be forced to disengage. Representatives from small and medium companies would be most impacted.

Ensure Fusion Centers Consistently Share All-Hazards Threat Information with the Private Sector

Conclusion 7: Chemical

Provide stronger DHS leadership of fusion centers or other local organizations. Improve consistency by issuing requirements and guidelines tied to Federal funding.

- Require an all-hazards threat approach, not solely law enforcement.
- Mandate sharing with the private sector and issue guidelines for outreach and communications.
- Introduce hiring and training standards to cultivate consistent analytical capabilities.

Conclusion 8: Chemical

Identify programs in existing fusion centers that work well with the Chemical Sector and use as models for other fusion centers operating in areas with a number of high-risk chemical facilities.

- Fusion centers present an opportunity to improve information sharing at the local and regional levels.

Develop a National Network of Chemical Sector Cyber Information-Sharing Communities

Conclusion 9: Chemical

Building on the SSA model, use the Industrial Control Systems Joint Working Group and US-CERT to share vulnerability and incident information to and from private sector security specialists and develop mitigation strategies. Leverage the US CERT network to distribute actionable mitigation information to smaller companies.

- Create a parallel structure to the network of security directors by designating a cyber security specialist at every chemical company and from equipment and software vendors.
- Build upon the ACC Cyber Incident Response Process, which provides cyber security officers a number to call with an anonymous cyber security incident and rapidly consult with other technology experts to determine the need to brief other companies and government partners for situational awareness.
- Use the SSA model to engage cyber security specialists in different technology or system specialties to share incident information that is relevant to them among themselves and with the Federal Government.
- Engage this network of owner/operators and vendors for Chemical Sector cyber briefings from the government.

Appendix D. Case Study: Commercial Facilities Sector

TABLE OF CONTENTS

1.0 Introduction

Overall, the Commercial Facilities Sector is well organized for security, and companies have collaborated effectively through industry associations and trade groups for many years. Most major companies within the sector are knowledgeable, engaged, and cooperative on security measures, due in part to a culture of working together on noncompetitive issues. These companies generally have good access to government threat and vulnerability information for both physical and cyber assets. By contrast, smaller companies are often less engaged in homeland security issues and may not be familiar with many of the information-sharing mechanisms that are available.

The Commercial facilities Sector has experienced clear improvements in information sharing over the past five years. Information-sharing mechanisms have matured and a strong relationship with the sector's Sector Specific Agency (Department of Homeland Security) has improved the quality and relevance of information provided to the sector. Yet despite these improvements, owners and operators are frustrated by the lack of understanding within government of their security information needs, insufficient coordination with and among government agencies, and deficiencies in information systems that sometimes fail to get the right information to the right people in a timely manner. The Commercial Facilities Sector believes that more needs to be done to streamline and simplify sharing mechanisms; to gather and disseminate threat data that is useful to the sector in bolstering security practices; to improve authority and accountability among Federal agencies responsible for sharing threat information; to remove confusing and duplicative information streams and reporting requirements; and to create formal and sustainable channels for partnership.

2.0 Sector Profile

Commercial facilities in the United States encompass a variety of mostly privately-owned establishments that typically encourage open public access without highly-visible security deterrents. Commercial facilities are ubiquitous; Americans work in, shop at, or visit many types of commercial establishments daily. Facilities range in size and design from small, single-site office buildings to massive parks, stadiums, convention centers, and retail establishments that can exceed five million square feet each. Because their design and function vary widely, commercial facilities are typically organized into eight subsectors that frequently work in partnership:

1. **Entertainment and Media**—Includes media production facilities, print media, and broadcast companies
2. **Gaming**—Includes casinos and the hotels, conference centers, arenas, and shopping centers associated with them
3. **Lodging**—Includes non-gaming resorts, hotels and motels, hotel-based conference centers, and bed-and-breakfast entities
4. **Outdoor Events**—Includes amusement parks, fairs, exhibitions, parks, and additional outdoor venues that host mass gatherings for temporary or permanent events
5. **Public Assembly**—Includes convention centers, auditoriums, stadiums, arenas, movie theaters, cultural entities, and additional assets where large groups meet and congregate
6. **Real Estate**—Includes office buildings and parks, apartment buildings, multi-family towers and condominiums, self-storage entities, and property-management companies
7. **Retail**—Includes any business that sells merchandise from a fixed location (e.g., shop, kiosk, mail, online) for direct consumption by the purchaser, as well as the locations (e.g., malls and shopping centers) where retail establishments are congregated

8. **Sports Leagues**—Includes the major sports leagues and federations

Commercial facilities are considered “soft” targets because they are prevalent and diverse, are open to public access, and deliberately avoid the use of highly invasive or stringent security measures. Owners of commercial facilities range in size from small, single-city companies to national companies to large multinational corporations, resulting in vast differences in the size and capabilities of their security resources. These characteristics can complicate both government and the private sector efforts to identify security threats and share practical security information. Getting the right information to the right people in a timely fashion presents significant challenges due to the diversity of the facilities, companies, and information needs that exist in different subsectors.

To understand the varied needs of commercial facility owners and operators, NIAC conducted 28 interviews that included industry leaders from across the sector who have information-sharing and security responsibilities, along with representatives from the Commercial Facilities Sector Coordinating Council (CFSCC), the Sector-Specific Agency (SSA), and the Federal Government and U.S. Intelligence Community (IC). Interviews included representatives of the several subsectors: Entertainment and Media (2), Gaming, Lodging, Outdoor Events (3), Public Assembly, Real Estate (10), Retail (2), and Sports Leagues.

Sector Makeup

The United States relies heavily on the economic vitality of commercial facilities. The Retail industry alone encompasses more than 1.6 million U.S. establishments and more than 24 million employees—accounting for one in five American workers. The retail industry conducted more than $4.6 trillion in sales in 2008. The Lodging industry generated $139.4 billion from travel in 2007 and the Gaming industry paid more than $5.7 billion in gaming taxes in 2008. Sports Leagues, including Major League Baseball, the National Football League, and the National Basketball Association, generated an attendance total of 118 million fans in 2008, and in the same year box office receipts for the motion picture industry (Public Assembly) totaled roughly $9.8 billion from an attendance of 1.4 billion individuals. In 2007, 341 million individuals visited amusement and theme parks (Outdoor Events), which generated $12 billion in revenue. An estimated nine million jobs in the United States are generated or supported by commercial Real Estate, which encompasses millions of establishments and constitutes about 13% of the nation’s gross domestic product by revenue. In 2009, the Lodging subsector included 50,800 properties (with 15 or more rooms), totaling 4,762,095 guestrooms, $127 billion in revenue, and $16 billion in pretax profits. (See Figure CF-1 for sample assets.)

Subsector and Cross-Sector Interdependencies

Due to its large size and diversity, the sector relies on multiple, smaller industry associations to facilitate information sharing, although there is substantial overlap and integration of security interests and responsibilities across the eight subsectors. For example, a Gaming establishment might contain facilities in the Lodging, Public Assembly, Entertainment and Media, Retail, and Real Estate Subsectors. This is true across other critical infrastructure sectors as well. The Commercial Facilities Sector houses or is co-located with critical assets—such as executive branches, back of house operations, and retail space—in other sectors (including Banking and Finance and Transportation) and manages operations and security for those employees. This frequently creates confusion over who owns the facility, who is responsible for security, and which information channels should be used to communicate threat information to the right people. One interviewee shared an example in which the Federal Government, assuming a bank was the owner of a high-profile building, contacted bank executives rather than the building owner about a building-related threat, thereby delaying the delivery of critical information to the company that manages security for the building. Likewise, the Federal Government occupies roughly

Figure CF-1. Sample Assets and Revenues in the Commercial Facilities Sector

The sector, valued at $6.7 trillion with $3.5 trillion in debt, encompasses a diverse array of assets, including:

- 53,500 hotels
- 46,400 shopping centers
- 125,000 schools (many more school buildings) and 14,500 school districts
- 1,600 stadiums and arenas
- 739,000 commercial office buildings consisting of 12 billion square feet of floor space
- 1,300 museums
- 200 theme and amusement parks

Sources: Commercial Facilities Sector-Specific Plan; DHS NIPP Snapshot: Commercial Facilities Sector; Meet the Target – The Lodging, Retail and Office Subsectors

80 million square feet of office and support space within privately owned and operated facilities throughout the United States—and those private companies usually are responsible for maintaining security of those facilities and employees.

Services provided by other critical infrastructure—including Energy, Water, Telecommunications, Emergency Services, Public Transportation, and Agriculture and Food (for restaurants housed in the Commercial Facilities Sector)—are critical to maintaining safety and operations for the Commercial Facilities Sector. The Commercial Facilities Sector relies on other essential vendors to maintain operations and security as well. Many companies contract for security services, building equipment operation, housekeeping, maintenance, and parking operations that employ staff who often become extended eyes and ears of a facility's security force.

The roles and responsibilities of people and entities within the Commercial Facilities Sector are not always clear to the government, to other sectors, or even members of the sector. For example, the role of the security director or manager can vary among companies. A contract security director might oversee security for an asset or a company, but defer to the property/facility manager who represents the ownership of the facility and has the necessary authority to take an issue directly to the government or to law enforcement. To mitigate confusion, use of the terms "security director" or "security manager" in this case study indicates the person who has custody of the property and responsibility for its care.

Operating and Security Characteristics

Unlike some critical sectors that employ substantial physical barriers to limit access and protect assets, commercial establishments typically encourage unfettered public access to most facilities for both business and personal purposes. Security teams must strike a balance to provide an open, economically active venue and the necessary security to protect all facility users and employees. Customer confidence in an establishment's security is critical to its economic viability.

The protection of assets in the Commercial Facilities Sector focuses both on physical and cyber security. Security teams, many of them contract employees, must deal with a diverse set of day-to-day security issues, including theft, vandalism, civil disturbances, and disease outbreaks ranging from influenza to food poisoning. Cyber systems aid daily operations and include retail trade credit card processing; access control card systems; loss prevention systems; fire and other intrusion alarms; communication centers; heating, ventilation, and air conditioning systems; and closed-circuit television monitoring. A widespread telecommunications failure poses the most severe cyber threat to the Commercial Facilities Sector.

Historically Targeted Sector

The relative ease of access to facilities and the potential for a successful terrorist attack to cause widespread fear and significant economic impact make commercial facilities attractive targets. As a result, security directors consider terrorism prevention to be among their primary responsibilities. Domestic and global terrorist attacks on commercial facilities have been successful. The World Trade Center in New York City, a commercial office and multi-use complex, was attacked twice. The February 26, 1993 attack resulted in six casualties and more than 1,000 injuries, with $1.6 billion awarded in damages. The September 11, 2001 World Trade Center attack resulted in 2,759 deaths, $7.7 billion in victim's compensation payments, and the destruction of a New York City icon. In a notable international attack, gunmen carried out a series of coordinated attacks across Mumbai on November 26, 2008, targeting the Taj Mahal Palace Hotel, Oberoi Trident Hotel, and Leopold Café. Approximately 173 individuals were killed and more than 600 injured during the 60-hour event. (See Figure CF-2 for a summary of these and some additional attacks on the Commercial Facilities Sector compiled from open source materials).

Figure CF-2. Commercial Facilities Sector Incidents

January 17, 2011 – Spokane, Washington – Kevin Harpham targeted the annual Martin Luther King Unity March and attempted to place a bomb along the planned route.

November 26, 2010 – Portland, Oregon – Mohamed Osman Mohamud targeted the Christmas tree lighting ceremony.

May 1, 2010 – New York City, New York – The Times Square attempted bombing occurred, with additional back up target locations including an iconic center in midtown Manhattan, a property located in lower Manhattan, and headquarters facilities in Connecticut.

September, 2009 – Dallas, Texas – Hosam Smadi tried to detonate a truck bomb in the garage beneath a Dallas skyscraper; the attack was foiled by the FBI.

July, 2009 – Jakarta, Indonesia – U.S. owned and operated J.W. Marriott and Ritz-Carlton hotels were simultaneously bombed in Jakarta's central business district, killing 7 individuals and wounding more than 50.

November 26, 2008 – Mumbai, India – Gunmen carried out a series of coordinated attacks including the Taj Mahal Palace Hotel; approximately 173 individuals were killed and 300 were injured.

December 5, 2007 – Omaha, Nebraska – Robert Hawkins attacked Westroads Mall, killing eight individuals and wounding four.

June 29, 2007 – London, England – Two car bombs were discovered in the Tiger nightclub incident.

September 11, 2001 – New York City, New York – Al-Qaeda terrorists hijacked and crashed two airplanes into the two World Trade Center Towers; approximately 2,759 individuals were killed with $7.7 billion in victim's compensation payments.

August 5, 2001 – Jakarta, Indonesia – A suicide bomber detonated a car bomb outside the lobby of a Marriott Hotel, killing 12 individuals and injuring 150.

February 26, 1993 – New York City, New York – Ramzi Yousef detonated a truck bomb in a parking garage under the World Trade Center complex, killing six individuals and resulting in $1.6 billion awarded in damages.

3.0 Commercial Facilities Sector Information Sharing Framework and Processes

Security Responsibilities and Information Needs

The largest companies in each of the eight subsectors typically own and/or operate multiple facilities across the United States and around the globe. These companies often employ a senior security director for all assets in the company, regional security directors for each geographic region, and security managers at each facility. This requires that owners/operators and security directors receive threat information at the facility and city level, as well as regionally, nationally, and globally.

Because most assets in the sector must be open and accessible to the public, physical security is extremely challenging and increases the sector’s dependence on information that will enable it to detect and deter threats to its assets. Security directors value detailed information about threats, such as targets, trends, pre-operational methods of operation, and attack methodologies. Such details enable security directors to make proactive changes such as changing security patterns, bolstering X-ray screening and surveillance procedures, and networking with neighboring properties/facilities.

A substantial number of security directors we interviewed indicated they prefer raw or fragmentary intelligence information (unfiltered or unscrubbed) over the finished intelligence products they typically receive. Many security managers are concerned that Federal intelligence analysts are unfamiliar with sector operations and may not recognize valuable details that the Commercial Facilities Sector would find useful to “connect the dots” regarding a potential threat. Such fragmentary information may be discarded by Government analysts because it does not fit into a finished piece of intelligence or because they do not realize its significance to the sector.

The Commercial Facilities Sector also requires cross-sector information to protect facilities that overlap with other critical sectors. Threat reporting concerning terrorist targeting of a specific financial institution, for example, is equally critical to the security director of the company that manages that institution’s office building, or the sports arena that bears its name.

The Commercial Facilities Sector relies on a variety of non-government sources because the information is often unscreened or unfiltered, and the content and quality of government-provided information does not fully meet the sector’s needs. The majority of individuals we interviewed prefer systems that “push” information to them because few have the time, resources, or capacity to regularly access multiple “pull” systems. One such system is the Department of Homeland Security (DHS) Homeland Security Information Network – Critical Sectors (HSIN-CS), in which users must navigate the system to locate pertinent information. In addition, HSIN-CS represents just one of many information conduits that the private sector uses to access government information. Minimizing conduits for all threat information will reduce confusion and duplication among competing and redundant Federal programs.

Commercial Facilities Sector Information Sharing Relationships

Most security directors we interviewed reported that personal relationships are paramount for effective information sharing and frequently serve as their primary source of threat information. Many security directors and their staffs come from a law enforcement or intelligence background and maintain their contacts when they move to the private sector. Connections are often leveraged using both formal and informal channels to share and validate information. Many noted that when they receive government information through a security bulletin or other formal channel, they often reach out to their personal contacts in the appropriate agency to validate, clarify, or augment the information. Personal contacts are equally important at the local level, where security directors are in close contact with State and local law enforcement for incident response and suspicious activity reporting.

Security directors also coordinate regularly with their peers from other companies to compare and share information on evolving threats and suspicious activities. In some cases, security directors worked with their contacts to form their own information sharing communities built around common security concerns, such as the Rockefeller Center Area Security Directors, which invites security directors to meet with local police each month. In many cases, such informal relationships have evolved into private-sector organizations or sub-groups of established industry associations, focused primarily on security and information sharing. These include the Real Estate Roundtable, the Real Estate Information Sharing and Analysis Center (RE-ISAC), the Building Owners and Management Association (BOMA), the Retail Industry Leaders Association (RILA), the American Hotel and Lodging Association (AH&LA), and National Retail Federation (NRF).

The Commercial Facilities Sector has adopted the National Infrastructure Protection Plan (NIPP) Sector Partnership model, under the Critical Infrastructure Partnership Advisory Council (CIPAC). The Commercial Facilities Sector Coordinating Council (CFSCC), made up of owner/operators in the eight subsectors, works closely with its counterparts in DHS, the Sector-Specific Agency (SSA) for Commercial Facilities. Several interviewees highlighted the effective leadership of the CFSCC as a chief reason for successful communication and collaboration.

Many security directors we interviewed know their DHS contacts and have had robust interactions with them in the past, though few saw them as a prominent source of threat information. Sector relationships with DHS have improved over time and allowed for more effective communication, coordination, and interaction. Several noted they had built a valuable relationship with their DHS Protective Security Advisor, whom many described as well-attuned to the needs of the Commercial Facilities Sector, but often spread too thin with responsibilities for all 18 critical infrastructure sectors over a large geographic area.

Key Information Sources and Mechanisms

Many of the security directors and managers we interviewed rely on a multitude of public and private sources to obtain information on threats, trends, and intelligence related to their security operations. The DHS Office of Intelligence and Analysis (DHS I&A) and the Federal Bureau of Investigation (FBI; including InfraGard) provide Federal intelligence and threat information at the national level. Information may be received through Federal Government contacts at industry association meetings, classified intelligence briefings, internet portals such as HSIN-CS, and through personal relationships. At the regional level, security directors said they look to both State and local fusion centers and local law enforcement in the jurisdictions where their key assets are located. Some security teams also turn to private companies, such as Michael Stapleton Associates, for domestic and local threat information. For international risk information, companies rely on the State Department’s Overseas Security Advisory Council (OSAC) and private companies such as TransSecure, iJet, Stratfor, and Control Risk. Some of the larger commercial facility companies have established their own intelligence gathering and analytic capabilities to mine information from a number of government, proprietary, and open sources and tailor it to their specific facility or company needs.

Industry associations and information-sharing organizations within the sector provide an invaluable network that security directors use to build relationships and exchange information among their peers. The Real Estate Roundtable, for example, was identified by many security directors as the focal point for information sharing within the sector because it brings together public and private institutions with major national influence to communicate and collaborate on relevant national policy issues. The Real Estate Roundtable maintains a Homeland Security Task Force, which champions the sector’s relationship with DHS and helps deliver relevant information from DHS to its members. In February 2003, the Real Estate Roundtable also organized the not-for-profit Real Estate Information Sharing and Analysis Center (RE-ISAC), which many have found to be a good conduit for disseminating information from government and reporting credible threats to the industry.

Other private-sector-managed associations serve similar roles for additional Commercial Facilities subsectors, including the Building Owners and Management Association (BOMA), the Retail Industry Leaders Association (RILA), and the American Hotel and Lodging Association (AH&LA). Many of these industry associations also contribute to the funding and operation of the Real Estate ISAC.

4.0 Effectiveness of Information Sharing in the Commercial Facilities Sector

Many commercial facility security directors agree that important progress has been made in information sharing between the Commercial Facilities Sector and the government over recent years, but much improvement is still needed. While they acknowledge that threat and risk information derived from Federal intelligence and reported through government channels is essential, they believe it is often not timely, actionable, accessible, or relevant.

Not Timely or Actionable

Interviewees commented that government information is often an after-the-fact analysis of an incident, arriving hours or days after it has occurred, or the incident has already been broadly reported by national news media—such as CNN, BBC, and Fox News—or local government groups (such as NYPD Shield). In these cases, Government information serves mainly to validate the accuracy of media and local government reports and perhaps provide additional context.

Several interviewees rely more heavily on commercial providers for information they feel is more timely, detail oriented, and actionable than what they receive from DHS and other Federal agencies. Intelligence products from private companies not only explain the relevance of the information to the Commercial Facilities Sector, but recommend basic mitigation and protective actions that allow security personnel and staff to enhance protection capabilities and response. Private services, however, can be costly and may be out of reach for companies with limited security budgets. A handful of security directors said that they would prefer to rely less on commercial providers but noted that such companies will continue to fill a niche until the government can deliver a comparable product.

Classified briefings from DHS Intelligence and Analysis (I&A) and other intelligence analysts had limited use for many of the security directors we interviewed because they did not provide timely, relevant, and actionable information. Those who have attended such briefings said they often left asking, “Why is this information important to me?” In many instances, “classified” briefings provided little information that wasn’t already in the public domain. When classified information is provided, security directors found that analysts focused on the source of the information or the manner in which it was collected rather than the specific vulnerabilities, targets, measures, means, and methods of operation. Many security directors interviewed said that they neither wanted nor needed to know information about intelligence sources and methods of collection.

One security director said classified briefings need to be simple, to the point, and provide direct instructions on what companies can do to bolster their security forces against emerging threats. Taking classified information, removing the specific sources, and disseminating the non-classified information to the broader commercial facilities community on a timelier basis would be more proactive and greatly increase the value of government intelligence information to owners and operators. It would extend the reach of valuable intelligence to those who do not have the necessary security clearances or are unable to frequently travel to Washington, D.C. where most classified briefings are held.

Hard to Access, Not Always Relevant

The difficulty in accessing Federal Government information causes private sector companies to turn to other sources. The complex and often redundant Federal information-sharing structure among Government agencies that have some counterterrorism or infrastructure protection mission leads to confusion about who security directors should contact for different types of information. The Federal Government emphasis on “pull” systems also hinders information sharing. Several people noted that HSIN-CS is cumbersome, difficult to use, requires frequent logins and password changes, and requires users to go in and actively search voluminous information on a wide range of topics in hopes of finding something useful (see Figure CF-3 for a specific example). There was a strong preference for “push” systems that send critical alerts out to the private sector. Interviews with Commercial Facilities SSA members indicated that recent redesigns of HSIN-CS provide improved functionality and customization that creates a push-type framework, but no private sectors users we interviewed were yet aware of those changes. The large amount of time it takes users to navigate HSIN-CS and find pertinent information often leaves security teams turning to private sector companies, which mine that information, analyze it, and provide it in a more actionable format.

Figure CF-3. HSIN-CS Incident Example

Many people we interviewed for this study expressed great frustration with HSIN-CS, including its access procedures, its confusing organization, and its lack of timely and meaningful content. One especially illustrative example occurred while Hurricane Irene was making landfall in the New York area in August 2011. The interviewee, a frequent HSIN-CS user with infrastructure protection responsibilities in New York, attempted to log on to the system for updates from emergency management agencies in the affected areas. Knowing that his password had expired, he entered it with the expectation that he would be sent to a page with the HSIN-CS Help Desk telephone number so that he could call it to change the password, as is the normal procedure. This time, however, he received an HTTP error message indicating that the website had denied him access but providing no further information. Unable to find the number online, he e-mailed a DHS representative who provided it and a quick call to the Help Desk reset the password. Using the new password, he again attempted to log in and again received the error message. During a second call to the Help Desk, the operator provided a series of instructions to erase the history in his Internet browser so that the log-in portal would grant access. The operator also provided a new log-in portal address as the old address had been discontinued.

After about 20 minutes, the interviewee was finally able to access HSIN-CS. He navigated straight to the Commercial Facilities Sector section of the website, but the most recent information that he could find on the hurricane was a three-day-old update plus links to the websites for FEMA and the National Hurricane Center, both of which the respondent had been using for days prior to the storm’s landfall. Clicking on a tab labeled “National Level Reporting,” he received the same HTTP error message that he encountered while trying to log in. Attempts to open compressed documents listed under a special “Hurricane Irene” tab soon proved cumbersome as each had to be downloaded to the interviewee’s browser and de-compressed prior to viewing to determine whether the document had information of interest to him.

Several others reported that the DHS-generated information they receive comes primarily through a relationship facilitated by the Real Estate Roundtable. Through roundtable members’ connections to the Federal Government, they help funnel information from DHS to owners and operators who might not access it from another source. They also help connect suspicious incidents among members who share information they have seen within this trusted group. While many in the sector view this as an effective model, several others recognized that those not being reached by the roundtable are missing out, particularly smaller real estate owners and operators and retail organizations.

Security directors also rely on local law enforcement information-sharing systems for threat and intelligence information. Law enforcement involvement and interest, however, varies by city. Some major cities have built trusted, established information-sharing relationships and mechanisms, while in others security directors say they find it difficult to get police departments to regularly communicate about or respond to suspicious activity. NYPD Shield, for example, sponsors e-mail notifications, web briefings, and periodic in-person briefings with the Commercial Facilities Sector. Their staff of analysts dedicated specifically to terrorism prevention pushes information out to the private sector, and is often faster at getting information analyzed and out than HSIN-CS or DHS I&A. However, this network is only accessible for security directors who oversee property in New York City—although the Real Estate Roundtable members share the information widely with the approval of the NYPD staff.

State and local fusion centers can provide another reliable source of threat and intelligence information. However, we found a wide variation in the level of interaction and the quality of information that owners and operators observed from different fusion centers. Some saw real value from fusion centers that have an explicit counterterrorism and/or CIP mission, and have adopted a model that closely integrates the private sector into the information sharing and analysis process. In the New Jersey Regional Operations and Intelligence Center (ROIC), for example, ROIC senior leadership and State Police meet quarterly with a private sector advisory group that includes representatives from the Transportation, Banking and Finance, Telecommunications, Energy, and Commercial Facilities Sectors. They share issues and information needs, and work on getting a better product to the private sector. What was once a series of one-off relationships turned into an industry-wide forum. But interviewees noted a lack uniformity and consistency in fusion center design. In some centers the roles and responsibilities are unclear and they don't provide much value to the private sector as a result. Several interviewees never had any contact with their fusion center or saw them as limited to being law enforcement bodies only. Despite this, nearly all security directors recognized the potential of these DHS-supported centers to serve as a critical hub for information sharing, provided they include both analysts and capabilities to meet the needs of specific critical infrastructure sectors. A number of security directors suggested that if a particular fusion center either does not have counterterrorism/CIP as a core mission or allow for private-sector participation, DHS funding to support those centers should be directed elsewhere.

Lack of Knowledge about the Commercial Facilities Sector

Perhaps the most common message from our interviews was that breakdowns in information sharing often occur because there is a fundamental lack of understanding about Commercial Facilities operations, responsibilities, and information needs by both DHS and the Federal Intelligence Community. Many believe that having dedicated analysts who have past experience in the Commercial Facilities Sector, or are tasked with learning about the sector and creating intelligence products designed to improve sector security, would significantly raise the value of government information. Although the diversity of the sector creates challenges in tailoring products to meet every need, having dedicated and knowledgeable personnel would greatly improve the effectiveness of information sharing.

We learned that a lack of knowledge about commercial facilities operations can lead to critical information not getting to the right individuals. Commercial facility assets are often deemed to be part of another sector. The individual businesses located within a building often do not own the property, yet government agencies mistakenly assume they are in charge of security when sharing threat information. Such misconceptions inhibit swift preventative actions and lead to poor coordination between Federal agencies and the private sector during incidents or potential threats (See Figure CF-4 for a summary of four specific examples).

Figure CF-4. Lack of Government Understanding of the Sector Hampers Threat Response

INCIDENT I:

An owner/operator of a commercial facility reported on a specific incident that highlights the lack of understanding of the sector by the government, the government's failure to share critical terrorism-related information with the private sector, and why many in the private sector rely on personal relationships with public-sector contacts rather than institutional ties.
In this specific incident, FBI agents came to a mixed-use commercial facility and wrongly assumed that the business they wished to communicate with was the landlord/property owner of the building. Once the proper owner of the building was contacted and able to meet, the FBI stated that they wanted to conduct a risk assessment of the property to examine vulnerabilities and to gain a better understanding of any specific risks. The individual representing the property agreed to allow the FBI to conduct the threat assessment but when they requested a copy of the final product, they were told that it would be classified.

The individual was able to use personal relationships to reach out to an FBI media contact in the public relations office of the FBI, who confirmed that partial plans of the building as well as other information were found on a recovered Al-Qaeda computer. This specific information was not provided by the FBI agents who came onsite or conducted the specific threat assessment. After receiving this critical information, the individual provided the FBI with access to the building tenants who were then interviewed, but still were not able to receive a copy of the assessment that was conducted.

The above example shows how a lack of understanding of the sector can hinder effective and timely information sharing. In this case, a credible and highly-specific threat against a property was discovered on an Al-Qaeda computer, yet the owner/operator of the facility was not apprised of the threat information and was therefore unable to strengthen the property's protective security measures. Only by reaching out to personal contacts in the FBI was the owner/operator able to determine that their property had been targeted. Additionally, the threat assessment that was conducted should have been provided to the property owner to allow them to gain situational awareness, take proactive security and mitigation measures, and provide critical information to their tenants.

INCIDENT II:

In the fall of 2010, intelligence officials briefed various private-sector owners and operators on the potential of a threat to a major metropolitan area. While this potential threat was identified as generic, and no specific target was identified, the FBI briefed a sports league that had games scheduled during the weekend on the threat information. However, it did not communicate the threat information to any other major sports leagues in the major metropolitan area, many of which also had events scheduled for the same timeframe. Also, there is no indication that the relevant stadium owners or operators were notified.
The above incident highlights a breakdown in coordination among government agencies in addition to the failure to warn all potentially affected private-sector organizations. In this case, the FBI elected to convey the threat information to the private sector itself rather than allowing DHS or another information-sharing mechanism to do so. While it did convey the threat information to one specific entity, it failed to disseminate the same information to others potentially affected.

INCIDENT III:

In late October 2010, intelligence officials in Saudi Arabia informed U.S. intelligence officials that Al-Qaeda in the Arab Peninsula (AQAP) had identified specific financial services companies and other entities as targets, and had modified explosives that were hidden in packages and sent to various executives' homes, designed to detonate when they reached their intended destination. These explosives were to be sent to the United States on international flights via UPS and FedEx. Intelligence reports further elaborated that UPS and FedEx packages carrying explosives had been mailed from Sana'a, the Yemeni capital, to Chicago via two airplanes with tracking numbers provided. The UPS cargo plane identified stopped in Qatar, then Dubai, where local officials discovered the IED inside a printer. The FedEx cargo plane stopped at East Midlands Airport in England, where the other device was found. Subsequent planes arriving in the United States (in Philadelphia and Newark) were searched, and in Brooklyn a UPS truck was stopped and inspected but no additional bombs or explosives were found.

(Continued)

Figure CF-4. Lack of Government Understanding of the Sector Hampers Threat Response (Continued)

While some financial services companies had been briefed about the potential threat, no general warning was provided to the broader private sector. Had the government done so, a wide variety of other potentially affected private sector entities could have taken appropriate security measures to screen incoming package deliveries and to potentially identify similar threats.

INCIDENT IV:

In June 2011, in the aftermath of the death of Osama bin Laden, Al-Qaeda posted a series of videos encouraging western Muslims to take up arms and conduct personal jihad in the United States and abroad. As a result of the videos, other internet users immediately responded with online activity that identified numerous commercial companies, organizations, and individuals as potential targets. Information from various Federal Government entities relating to the names of groups and individuals differed as to the exact list. DHS contacted private-sector partners to discuss the videos and stated that that it would share the names of the targeted parties with the sector following "duty to warn" contact by the FBI to the individually-named groups/persons. In the absence of timely information from either DHS or the FBI as to the identities of the companies and individuals listed, private-sector security personnel compiled an "unofficial" list which was then shared among owners and operators.

During a meeting between a senior FBI counterterrorism official and a member of the Commercial Facilities Sector approximately 10 days following release of the Al-Qaeda videos, the issue of timely warning of all potentially at-risk companies and individuals was discussed. While the private-sector partner conceded that the FBI had a duty to warn those parties specifically named in the Al-Qaeda videos, he noted that building owners and operators of multi-tenanted buildings where the targeted companies and individuals worked needed to be warned as well so that appropriate security measures could be instituted. Without notification from the government, however, the owners and operators would be ignorant of the threat to their properties and would not be able to take appropriate protective measures. The government's failure to contact all affected parties, including the owners and operators of the properties in which the purportedly targeted individuals and companies were housed, seriously compromised their ability to detect and thwart potentially hostile actions against the tenants in their buildings.

Sector Willingness to Share Information

Most security directors and managers in the Commercial Facilities Sector are quite willing to share suspicious activity and threat information with the government and regularly do so. One interviewee indicated that the private sector has an obligation to share that information, noting that threat and security information is non-competitive within the sector. Interviewees reported they frequently share threat information among their peers through trusted informal networks and personal relationships. Many security directors reported they frequently engage the facility's contracted vendors and staff—including security guards, parking attendants, housekeeping and maintenance staff—to serve as eyes and ears reporting suspicious activity throughout their facilities. By training and informing these individuals, and giving them clear instructions on how to report activity, they extend the reach of security capabilities across properties.

There are times, however, when private companies may withhold proprietary information to protect themselves and to keep their competitive advantage. Isolated incidents where information was misused—such as one in which a fusion center and law enforcement agency released all suspicious activity reports from one security director to a media reporter in response to a Freedom of Information Act (FOIA) request—can make companies hesitant to share company-specific information with the government. (Suspicious activity reports are protected from FOIA requests.) Government organizations can also create confusion about who should first receive suspicious-activity information and how it will be subsequently shared throughout the government. For example, suspicious-activity observed in parking operations would be reported to the DHS Transportation Security Administration, while suspicious activity at the building entrance would be reported to the DHS Office of Infrastructure Protection (DHS IP).

Several interviewees expressed great frustration at the lack of feedback from their government partners when they do share information, especially suspicious activity reports. One interviewee noted that information shared with the government "goes into a black hole" and the submitter is never told whether the information was received, evaluated, or assessed to pose a real threat (see Figure CF-5 for a specific example). Many saw feedback from the government as the only incentive to continue this information sharing process and noted that receiving no response is likely to de-motivate individuals to continue the practice.

Figure CF-5. Lack of Government Feedback Reinforces Reliance on Personal Relationships

On or about May 1, 2011, after the reporting of the death of Osama Bin Laden, an FBI office received an anonymous write-in e-mail threatening to detonate explosives at numerous named sites around the United States. The e-mail was not deemed credible by the Special Agent in Charge, due to the syntax and vocabulary of the message (the author was assessed to be a non-native speaker) and because he "has seen so many of these that he deemed it non-credible," one interviewee reported hearing. Industry sources, not the FBI, conducted additional investigation to this potential threat and 13 named locations (identified as "castles") located around the United States were specifically identified.

On May 2, 2011, a local FBI representative alerted a security director within the Commercial Facilities Sector to the threat and informed him that the FBI deemed it non-credible. It is unclear whether any other private sector partners were alerted at this time. Also around this time, an industry partner received a tip from DHS that there was "something going on and that the FBI was briefing hotels on a threat."

In early May, a hotel contacted their local police to report a suspicious package that had been left on their loading dock. According to industry sources, the package originated in Pakistan and was addressed to the general manager of the hotel. It was not an explosive device but, rather, a box containing mini-basketballs. The purpose of the package is still unknown at this time—no one at the hotel ordered the merchandise. The local police speculated that it may have been related to the FBI threat. The security manager on scene was unaware of the FBI threat, as were hotel personnel.

Private sector partners began to share information among themselves when the government was not doing so. Although the FBI e-mail threat contained named targets, the bureau only notified one security manager—who then contacted other entities that were specifically identified. The designation of the email threat as "non-credible" was likely correct, but was not reevaluated in light of the suspicious package incident because the information was not shared effectively. Owners at targeted facilities were not given the opportunity to increase their situational awareness or protective measures in response to the potential threat.

A poor understanding of commercial facility risks, combined with minimal follow-up to suspicious activities, can impair the ability of law enforcement and Federal Government agencies to act on time-sensitive information regarding potential terrorist activities or threats. Two examples emerged in our interviews (see Figure CF-6 for these specific examples) in which the private sector passed information to law enforcement or the Federal Government, and their failure to act on the information could have permitted a terrorist act to occur.

Figure CF-6. Current Information Sharing Does Not Support Rapid Response

INCIDENT I:

We interviewed the owner/operator of an internationally recognized, high-profile mixed-use commercial facility frequented by millions of people annually, who related an information-sharing attempt that highlights the challenges the private sector often experiences in bringing potentially important, time-sensitive information to the government's attention.

Recognizing that its facility presented an extremely high-value soft target to terrorists, the owner/operator's security department inaugurated in 2005 a surveillance detection capability using Behavior Pattern Recognition techniques to detect individuals engaged in surreptitious activity. At that time, the facility's security director met with local law enforcement to determine whether they would be prepared to respond in the event that suspicious activity was detected. He was informed that they would not, as "acting suspiciously" was insufficient grounds for detaining and interviewing an individual.

On the date in question, a patron of the facility alerted security personnel to the activities of an individual who he believed was secretly photographing portions of the facility. The surveillance detection team deployed and confirmed that the individual was engaged in clandestine videography of the layout of the facility, the ventilation system, and other suspicious areas.

Given that local law enforcement had indicated that it would not respond to such incidents, the security department interviewed the individual who claimed to be attending a nearby conference. An Iranian citizen and resident of the United Kingdom, he initially denied having been in contact with any other persons at the facility but recanted after being confronted with the fact that closed circuit television coverage showed him in contact with a group of individuals who subsequently dispersed throughout the facility. (He claimed that the others were attendees of the same conference but that he did not actually know them.) Following the interview, the suspect returned to his rental car and departed the facility.

The security department reported the above information to the local FBI office. No action, however, was taken. Separately, the patron who had initially brought the suspect's activities to the attention of the security department was sufficiently concerned that he called a personal contact at FBI Headquarters in Washington and reported the incident. FBI Headquarters then contacted the local FBI office to inquire as to the status of the investigation but was told that there was no investigation under way. Several days later the local FBI office contacted the security director at the facility and inquired as to why the incident had not been reported. The FBI office was told that the incident had, in fact, been reported at the time the incident occurred but that there had been no follow-up by the FBI. Subsequent investigation by the FBI indicated that the suspect was of counterterrorism interest.

This incident highlights the inability or possible reluctance of law enforcement and Federal counterterrorism agencies to act on time-sensitive information regarding potential terrorist threats provided by the private sector. Whether the local police department or FBI office felt that the information was of dubious credibility is unknown.

INCIDENT II:

The owner/operator of an internationally recognized commercial facility reported another attempt to share information concerning possible terrorism-related activity with the government. This high-profile commercial facility is routinely visited by tens of millions of U.S. and foreign visitors each year and the owner/operator recognizes that it represents an extremely high-value target to terrorists. Recognizing its status as a high-value soft target, the security department has implemented programs to identify potential threats and indicators of terrorism or other malevolent acts. The owner/operator also communicates regularly with both local and Federal law enforcement entities.

In this particular incident, a guest of the facility as well as security personnel identified three individuals who were covertly video-taping pedestrian bridges that are crossed by thousands of people on a daily basis. The individuals filming the bridges departed the premises prior to being questioned by security personnel, but their vehicle was identified and traced back to a different city. Before the FBI was able to follow up concerning this information, two of the individuals departed the country and a third individual to date has still not been accounted for.

This incident highlights the fact that information sharing is currently not agile enough to move at a rapid pace and that communication breakdowns continue to contribute to this problem. By the time that the local FBI office was able to communicate with the FBI office where the vehicle was traced to, two out of three of the suspect individuals had departed the United States. Additionally, the response and support of the second FBI office was unenthusiastic as it apparently considered the case outside of its geographic area of jurisdiction.

5.0 Findings

Based on our original interviews and open-source research, the members of the Commercial Facilities Sector Case Study team developed eight findings that summarize the status of intelligence information sharing in the Commercial Facilities Sector.

Finding 1: Commercial Facilities

DHS has been given primary responsibility within the Federal Government to share intelligence-derived counterterrorism and critical infrastructure protection information with the private sector, including the Commercial Facilities Sector, and has all of the necessary legal authorities to do so. DHS' implementation of programs and mechanisms to undertake this mission, however, has been slow to mature.

Although some believe that DHS does not have the necessary authorities to share intelligence information with the private sector, this is not the case. The Homeland Security Act of 2002, the Implementing the Findings of the 9/11 Commission Report Act, and numerous Executive Orders and Presidential Directives give DHS clear authority to serve as the principal conduit for information sharing with the private sector.

The implementation of effective information sharing programs and mechanisms has not been fully effective, however, in part because DHS lacks both full understanding of sector information needs and substantive intelligence expertise. As DHS was establishing its intelligence collection requirements, analysis, and dissemination procedures, it may not have received all of the guidance and oversight that it needed from the U.S. Intelligence Community (IC), whose resources were stretched as the Government entered the Global War on Terror. The Office of the Director of National Intelligence (ODNI) was established in 2004 to unify IC operations, and is now in a position to reevaluate and help revise DHS's intelligence programs to ensure their consistency with established IC processes and procedures.

In addition, despite the best intentions and diligent efforts of dedicated DHS staff members assigned to interface with the private sector, it is possible that DHS leadership may not have fully exploited and executed the explicit "authorities" DHS has been given.

Finding 2: Commercial Facilities

DHS has not effectively leveraged its role as the Sector-Specific Agency for the Commercial Facilities Sector, either by advocating for the information needs of the sector within the Intelligence Community or by developing more in-depth knowledge of how the sector works in order to provide the private sector with more focused, relevant analytical products.

The Commercial Facilities Sector expects DHS to disseminate CIP information to the private sector, and to advocate for the sector's information needs within the IC. The intimate understanding of sector operations and the longstanding relationships enjoyed by other critical sectors and their assigned Sector-Specific Agencies does not exist within the Commercial Facilities Sector. To more effectively serve as the Commercial Facilities SSA, DHS will need to develop deeper expertise in sector operations and more effectively articulate sector information needs to the IC.

Finding 3: Commercial Facilities

While DHS clearly has the mission to share information with the private sector, its lack of "ownership" of that information at times hinders its ability to carry out this function.

Although DHS is responsible for sharing intelligence information with the private sector, it can only do so if the "originating" Federal agency that collected the intelligence concurs. Because DHS's intelligence analysis capabilities are still maturing, it may not be viewed as a full partner within the IC and may not be an effective advocate to ensure that valuable information gets shared with the private sector. In addition, the information that the originating intelligence agencies provides to DHS is often already analyzed and filtered, which provides DHS analysts little or no context and which excludes potentially valuable but fragmentary CIP information from being shared with private-sector owner and operators who may recognize the value of the information when the government does not.

Finding 4: Commercial Facilities

Redundant information-sharing programs by various Federal agencies confuse and frustrate private sector users as they attempt to navigate an overly complex information sharing landscape. As a consequence, many have turned to private companies, industry associations and trusted personal contacts, within and outside of government, to meet their CIP information needs.

An overly complex Federal information-sharing landscape with apparently competing and redundant information-sharing programs has compelled many companies to hire their own analysts or to contract with private information providers to obtain relevant counterterrorism and CIP information. Some sector interviewees expressed a desire for a "one-stop shop" for information exchange with the Government and indicated that it is often unclear what the appropriate engagement points of contact are with Federal agencies. Additionally, the private sector is often overwhelmed with redundant information requests from multiple Federal agencies and programs during an incident.

Personal relationships, including participation in private industry associations, are seen as paramount for effective information sharing and delivery. Many security directors also cite successful preparedness and information sharing relationships with local law enforcement, often built on established relationships from their prior law enforcement, government, or intelligence experience.

For the Commercial Facilities Sector, systems that push information out to the sector are far more valuable than those that require pulling information from a government source (e.g., HSIN-CS), which is seen as unnecessarily time consuming, cumbersome, and hampered by technology issues.

Finding 5: Commercial Facilities

The Federal Government lacks an operational understanding of the information needs of the Commercial Facilities Sector and its subsectors, and it tends to: 1) share information that is not relevant, practical, or useful; 2) filter out information that could be of value to the sector; and 3) hold classified briefings that provide limited or no value.

Government information is rarely specific, practical, or relevant, and the Commercial Facilities Sector looks to other forums to obtain forward-looking intelligence that helps security directors and their teams take anticipatory infrastructure-protection actions at their facilities. The sector's eight subsectors rarely operate independently of each other. A lack of government understanding of both intra-sector and cross-sector assets and their impacts may prevent the sector from receiving relevant threat information.

Many in the Commercial Facilities Sector prefer to receive unfiltered information rather than finished intelligence disseminations, because they fear that the government's lack of sector understanding may lead to finished intelligence products that may leave valuable data and details "on the cutting room floor." The sector also feels that classified briefings focus on unnecessary source information and do not typically provide information that is of most value: vulnerabilities, targets, trends, and methods and means. Classified briefings are seen as providing no more information than what has already been reported in the media or is otherwise available in open-source materials.

Finding 6: Commercial Facilities

Sector owners and operators are willing to share incident or suspicious-activity information with the government, but are frequently discouraged because the government provides little or no feedback indicating 1) whether the information was valuable, 2) that it was investigated or acted on in a timely manner, or 3) whether or not it could signify a threat to the sector.

Without a formal feedback process in place, the government frequently does not "close the loop" with the private sector on the information it provides. Owners and operators often must turn to their personal contacts within government to determine whether the information was received, evaluated or indicates a potential threat to their company. Because the government does not appear to evaluate or act on private-sector information in a timely manner, many owners and operators believe that the government generally does not value the information they provide.

Some level of government feedback to the private sector is critical to encourage continued sharing and enable security teams to refine their information-collecting processes to report the type of information government finds most valuable. Security managers also use feedback to close the loop with members of their security team—who often witness and report incidents first hand—on whether reported information indicates a threat or requires action.

Finding 7: Commercial Facilities

Fusion centers do not consistently have counterterrorism or critical infrastructure protection (CIP) missions, or engage the private sector in information analysis and dissemination.

The design and operation of each fusion center is largely determined by the entity in charge and how the center was originally conceived. For example, some are operated by the State Police and were created strictly for law enforcement purposes that do not include counterterrorism or CIP. Also, because there is no central coordinating authority for fusion centers, the State/local fusion center model does not work for private-sector companies that manage security out of a head/national office. The 72 fusion centers provide no coordinated threat picture and communicating regularly with all applicable fusion centers is impractical.

Security directors in the Commercial Facilities Sector have shown an interest in actively building relationships with local law enforcement and fusion centers. While this study found that not all fusion centers have counterterrorism and/or CIP as a mission, those that do often succeeded in providing valuable outreach and communication with the private sector.

Finding 8: Commercial Facilities

The Commercial Facilities Sector recognizes the value of engaging extended staff and contractor resources in security operations under the "See Something, Say Something" model.

Incorporating extended staff and contractor resources in security operations brings a recognized value and sophistication to the security approach. A number of Commercial Facilities Sector owners and operators engage their maintenance, cleaning, parking, and service staff and vendors in their security operations as a best practice, and provide training in multiple languages to ensure that all are aware and educated on specific threats and related indicators.

6.0 Conclusions

The structure and makeup of the Commercial Facilities Sector sets it apart from other sectors in its information-sharing requirements and its relationship with DHS. The range of sector facilities, including sporting events, theme parks, commercial office buildings, casinos, hotels, shopping malls, and retail establishments, operate almost exclusively on an open-access model in which large numbers of people congregate in public venues where stringent security measures are neither desirable nor practical. As such, the sector includes many high-value soft targets for terrorist groups whose goals are to cause mass casualties and severe economic disruption. The Commercial Facilities Sector has, in fact, been the single most frequently targeted and impacted of the 18 critical infrastructure sectors.

The Commercial Facilities Sector believes that structural and programmatic changes within DHS are needed to improve the efficacy of DHS's information-sharing mission. If it is deemed that DHS cannot become a more effective information-sharing partner with the Commercial Facilities Sector within a reasonable amount of time, the sector believes that the Administration should consider whether another Federal agency may be a more suitable organization to fulfill this role.

Given the unique structure and characteristics of the Commercial Facilities Sector as well as its constantly being a potential terrorist target, the members of the Commercial Facilities Case Study team believe the following 10 conclusions are most important for improving information sharing between the government and the sector.

Conclusion 1: Commercial Facilities

ODNI must take a leadership role in assisting DHS to develop more systematic, relevant, and timely information sharing programs and mechanisms. DHS, in its role as a communicator but not an originator of threat information, must become a more credible and effective member of the IC, and it must be empowered and accepted by the IC in order to carry out its information-sharing mission.

ODNI should take a direct and active role in assisting DHS to develop effective, relevant, and timely information-sharing mechanisms for the Commercial Facilities Sector and ensure that the CIP intelligence collection requirements, analysis, and dissemination procedures are consistent with those already in place in the IC. To fully realize its mission of sharing critical threat information with the Commercial Facilities Sector, DHS must be empowered to safely share threat information produced by other IC components with cleared private entities. To do so, ODNI should:

- Proactively ensure that intelligence the IC collects that has potential CIP ramifications is released to DHS for dissemination to the private sector in a timely manner. DHS is charged with disseminating CIP intelligence but it is rarely, if ever, the originating agency. Because it typically does not "own" the information, it is powerless to disseminate it, even to cleared private-sector partners, unless the originating agency agrees. This can be a lengthy and time-consuming process which can hinder the effectiveness and intent of the information-sharing process.
- Establish cells of collocated IC analysts, DHS I&A and DHS IP personnel, and cleared private sector critical infrastructure experts within the National Counterterrorism Center (or another appropriate IC component) to assume primary Federal responsibility for identifying threat information for the Commercial Facilities Sector. DHS and ODNI personnel should develop the analytical capabilities and Commercial Facilities Sector expertise to deliver proactive intelligence products that enable owners and operators to take anticipatory security steps and countermeasures to protect critical-infrastructure assets. The cells should conduct "red team" assessments of potential threats to critical-infrastructure assets that the Commercial Facilities Sector can use in developing their security programs. Private-sector analyst participation is essential and a similar model should be considered for other sectors.
- Review existing DHS information-sharing programs and revise them as necessary to ensure that they provide timely and relevant intelligence-derived counterterrorism and CIP information to the private sector.

- Develop new intelligence-dissemination products tailored to private-sector CIP information needs, including fragmentary information from raw reporting, and provide greater insight into the assessed credibility of the information.
- Assist DHS in developing standardized distribution lists for CIP information to ensure that all critical sectors are informed of potentially relevant counterterrorism and CIP information in a timely manner.
- Commission a classified National Intelligence Estimate (NIE) of the assessed capabilities and intentions of terrorist groups to target critical infrastructure assets in the United States. The NIE should consider terrorist threats to all 18 critical infrastructure sectors and it should identify those groups assessed as potential threats, specify their likely methods of operation and, if possible, assess the potential vulnerability of individual sectors to such attacks. No declassified version of the NIE should be made public, although the classified version should be shared broadly with those appropriately-cleared individuals in each sector who have bona fide infrastructure-protection responsibilities.
- Assume an active role in the DHS Standing Information Needs requirements-generation process, ensuring that core intelligence collectors throughout the IC receive critical infrastructure collection requirements solicited from the critical-infrastructure sectors at least on an annual basis. DHS must work with the IC to ensure that those requirements are accorded appropriate priority among competing intelligence requirements and that core collectors and analysts are rewarded for recognizing and disseminating CIP information to the private sector. A mechanism to convey short-fused or ad hoc requirements from the private sector to IC collectors should also be established.
- Assist DHS to develop meaningful counterterrorism analytical expertise by requiring mandatory rotational assignments of DHS analysts to other IC counterterrorism analytical components as a prerequisite for promotion to supervisory positions, and ensure a robust rotational program of experienced IC counterterrorism analysts and senior managers to DHS.

Conclusion 2: Commercial Facilities

To further leverage its role as the SSA for the Commercial Facilities Sector, DHS should establish a robust rotational program that brings in private sector analysts from the Commercial Facilities Sector to work alongside DHS I&A and DHS IP personnel and provides opportunities for DHS analysts to participate in rotational assignments at sector security and intelligence departments.

By exposing DHS analysts to the expertise both of Commercial Facilities Sector operations and private-sector security analysts, they can develop meaningful Commercial Facilities sector knowledge needed to make them a more effective partner.

Conclusion 3: Commercial Facilities

The Commercial Facilities Sector would prefer that the Administration reduce the number of information-sharing conduits from the government to the private sector, with a more concentrated number streamlining information delivery and improving its efficiency and relevance.

The Commercial Facilities Sector believes that the current content and quality of threat information from the government does not meet the sector's needs. Furthermore, the sector feels that there are currently too many government conduits of information that they have to access to ensure that they are getting all of the information relevant to their infrastructure-protection responsibilities. Reducing the number of existing conduits of threat information will minimize confusion and duplication among competing and redundant Federal programs. The Commercial Facilities Sector believes that these identified conduits should be based on a “push” model, where important information is actively disseminated to recipients, as opposed to a “pull” model that requires recipients to seek out information from Federal Government websites.

Conclusion 4: Commercial Facilities

Assuming that HSIN-CS continues as the preferred information-sharing conduit for the government to the critical infrastructure owners and operators, DHS should commission an outside, independent evaluation of the efficacy of its current design and redesign it as necessary to make the information it provides more accessible, the paths to the information more intuitive, and its navigation less confusing to users.

The existing HSIN-CS does not meet the needs of the Commercial Facilities Sector and has been rendered largely irrelevant due to its confusing structure, organization, and complex user interface. DHS should look to the Department of State’s OSAC website as a potential model for an effective information-sharing mechanism to communicate threat information to the private sector.

Conclusion 5: Commercial Facilities

DHS IP and DHS I&A must work together more effectively as partners in the information sharing process; or if they are unable to do so, the Administration should consider recombining these two offices, as was the original intent of Congress.

As envisioned by Congress in the Homeland Security Act of 2002, DHS IP and DHS I&A were combined in a single office to provide both intelligence and infrastructure protection support directly to the 18 critical-infrastructure sectors. The offices were subsequently separated to ostensibly improve efficiency, but this separation has contributed to significant problems in information sharing. From a customer-support perspective, DHS leadership should reassess the logic and efficacy of separating DHS IP and DHS I&A, specifically whether the current separation best serves the needs of critical-infrastructure sectors (including the Commercial Facilities Sector) for timely and efficient information. If DHS is unable to resolve these issues, the Administration should consider recombining the two offices to improve efficiency.

Conclusion 6: Commercial Facilities

DHS should programmatically administer Federal counterterrorism and critical infrastructure protection (CIP) support to fusion centers, making the provision of Federal funding contingent on each fusion center’s adoption of counterterrorism and CIP as a core mission, sharing such information with private-sector critical-infrastructure partners, and ensuring private sector access and participation.

Because not all fusion centers have counterterrorism and/or CIP as core missions, not all should benefit from DHS funding intended to enhance counterterrorism and CIP programs. DHS should designate or establish a component within the Department to assume programmatic responsibility for administering counterterrorism and CIP support to fusion centers. DHS should segregate funding from funds intended for other purposes, including general support to local law enforcement, all-hazards disaster response, etc., and make the provision of funding contingent on each fusion center’s commitment to a legitimate counterterrorism and CIP mission, its private-sector information-sharing activities, and its embrace of private-sector access and participation. The component should standardize counterterrorism and CIP mission requirements and performance standards across fusion centers, ensure that the local threat level and critical infrastructure assets appropriately guide the allocation of resources, facilitate the dissemination of information from the Federal Government to the fusion centers as well the sharing of information among fusion centers, and evaluate the efficacy of funding in enhancing local CIP. In addition, DHS should encourage coordination between the local Joint Terrorism Task Forces (JTTFs) and the relevant fusion centers to ensure that appropriate information is shared among them and that a common threat picture is conveyed to the private sector when circumstances dictate.

If any given fusion center does not have a counterterrorism or CIP as a core mission or if it does not facilitate active private-sector participation, DHS should redirect counterterrorism and CIP funds from that fusion center to other programs that enhance the private sector's critical-infrastructure-protection activities.

Conclusion 7: Commercial Facilities

DHS should establish a centralized mechanism, such as a National Fusion Center, to enable companies with broad geographic infrastructure-protection responsibilities to obtain information from a single source as opposed to requiring them to interact with multiple geographically based fusion centers.

The current fusion center structure does not allow non-government organizations with broad geographic infrastructure protection responsibilities to obtain information from a single source, requiring them to instead establish separate relationships with multiple fusion centers.

Conclusion 8: Commercial Facilities

DHS should develop a formalized process and necessary protocols to provide timely feedback and follow-up information to the sector when it shares suspicious activity reports (SARs) and other threat information.

Many security directors in the Commercial Facilities Sector reported frustration by the lack of feedback from DHS when it shares potential threat information. Security directors need to know if and when the government followed up on the information, and whether or not it could indicate a threat for the sector or a facility. By providing feedback, DHS can help the sector understand what information is valuable and encourage it to continue sharing.

Conclusion 9: Commercial Facilities

DHS should share critical infrastructure protection and counterterrorism information with the extended contractor and vendor communities within the Commercial Facilities Sector.

A key information sharing “success factor” within the Commercial Facilities Sector has been to harness extended staff and contractor resources in security operations. Security, maintenance, cleaning, and parking operations personnel, service staff, and vendors can serve an invaluable security function as they are often the individuals who first notice suspicious activity.

Incorporating extended staff and contractor resources in security operations brings a valuable force multiplier to the protection of CIP assets and should be applied throughout the Commercial Facilities Sector as well as the other critical infrastructure sectors.

Training materials should be created and shared in relevant foreign languages to the contractor population to best engage all staff members relating to the potential programs (e.g., active shooter training materials created in both English and Spanish).

Conclusion 10: Commercial Facilities

The government should facilitate the retention or reactivation of security clearances as cleared government personnel transition to CIP positions in the private sector, and it should leverage those trusted relationships to enhance the communication of counterterrorism and CIP information between the public and private sectors.

Significant numbers of formerly cleared Federal, State, and local government employees have moved to the private sector to assume responsibilities for the protection of critical infrastructure assets in the critical infrastructure sectors. The government should make a concerted effort to facilitate the retention or reactivation of clearances for these individuals and leverage these trusted relationships to the mutual benefit of both public and private sectors.

Many companies are willing to invest in this relationship by purchasing approved secure communication equipment, submit personnel to the intrusive and time-consuming clearance process, and fund their active participation if required.

Appendix E. Case Study: Healthcare and Public Health Sector

TABLE OF CONTENTS

1.0 Introduction

Many sectors rely on Healthcare and Public Health Sector assets and services for resilience in the face of threats—and its complex systems, networks, services, facilities, functions, and roles are essential to prevent disease and disability, treat patients, and foster public health. The security of critical Healthcare and Public Health Sector infrastructure, such as its trained workforce and established supply chains, greatly depends on the effective flow of intelligence information. The Sector is less well-organized for physical security and asset protection than it is for security of information and resilient, adaptable service delivery. Small and to some extent even large healthcare organizations and businesses depend substantially on trade associations and other networks for information sharing, and may seek and act on needed information with little or no government involvement.

During the past several years, the Healthcare and Public Health Sector has worked successfully with its Sector-Specific Agency (SSA), the Department of Health and Human Services (HHS), to improve the relevance of classified briefings and to provide intelligence information to Sector owners and operators through formal mechanisms such as the Homeland Security Information Sharing Network (HSIN). Much information in the Healthcare and Public Health Sector is proprietary, sensitive for business or regulatory reasons, or legally protected, hindering the success of efforts to establish a culture of information sharing. Despite significant advances, Sector owners and operators believe that government agencies inadequately understand their information needs, and that requests for information are often ignored. Members of the Healthcare and Public Health Sector believe that more can be done to improve intelligence information flow both to and from government entities.

2.0 Sector Profile

The Healthcare and Public Health Sector plays a vital material, symbolic, and economic role in the nation's well being. It includes goods, services, personnel, facilities, databases, financial systems, and surveillance functions; and it is comprised of public as well as private components.

The private side, 85% of the Sector, provides most clinical care and mortuary services, and produces medical products including drugs, biologics, and medical devices. The public side provides some clinical services, participates in ongoing surveillance and threat detection, finances private-sector efforts, and funds and operates most public health programs via Federal, State, local, territorial, and tribal health agencies.

Key Sector assets include healthcare delivery and research facilities; supply stockpiles; manufacturing and distribution centers; and cyber systems serving data storage, health surveillance, and insurance and payment processing purposes. The Sector's economic role is substantial and growing: in total, national health expenditures totaled $2.5 trillion in 2009, constituting 17.6% of U.S. Gross Domestic Product (GDP).

The Healthcare and Public Health Sector's six subsectors are:

1. **Direct Health Care**—Includes medical treatment facilities, State and local centers for the aging, nursing homes, rehabilitation centers, and group homes; personnel include doctors, nurses, pharmacists, dentists, emergency medicine and other clinicians and practitioners.
2. **Health Plans and Payers**—Includes health insurance, other third-party payers, and health plans that provide insurance coverage to both individuals and employers.
3. **Pharmaceuticals, Laboratories, and Blood**—Includes pharmaceutical manufacturers; pharmaceutical suppliers and distributors; laboratories and laboratory support services separate

from medical treatment facilities; hospital and community blood centers; transfusion services and transplantation centers; and individuals involved in activities related to transfusion, cellular therapies and transplantation medicine.

4. **Medical Materials**—Includes manufacturers, suppliers, and distributors of medical supplies and equipment, as well as health care materials managers.
5. **Mass Fatality Management**—Includes providers of services needed after death: medical examiners, coroners, funeral directors, cremationists, cemeterians, clergy, and manufacturers and distributors of funeral, memorial, and cremation supplies.
6. **Health Information and Medical Technology—**Includes the individuals and organizations that design, manage and implement all Sector Information Technology (IT) systems and capabilities, and the networks that support delivery of healthcare services.

These subsectors are linked by networks that disseminate clinical and public-health information, and they work together daily to manage supplies, provide clinical care, manage patients and payment processes, work with mortuary services, and respond to major natural disasters or terrorist attacks.

The Healthcare and Public Health Sector is highly interdependent with other sectors. The Agriculture and Food, Transportation, Energy, Water, Emergency Services, Information Technology, and Communications Sectors provide products and services that support essential Healthcare and Public Health Sector operations. The Sector's goods and services are provided within a complex web of regulations, policies, and financial and technical constraints. Furthermore, rapid expansion of health information technology and increasing reliance on these IT systems for health and insurance claims data have increased Sector vulnerability to cyber incidents.

The Healthcare and Public Health Sector depends heavily on both domestic and international manufacturers for critical supplies and raw materials. Medical providers depend on complex supply chains that can involve multiple vendors, sole-source manufacturers, international borders, and rare sources of raw materials, all of which cause particular vulnerabilities for the Sector and increase the challenge of meeting unanticipated demands. Diseases as well as medical supplies often travel freely over State and national borders, creating vulnerabilities to foreign supply-chain disruptions as well as to broad-ranging patterns of illness. For example, the April 2009 H1N1 influenza pandemic renewed concerns over international medical supply chains and vaccine availability. [46] The Sector must rely on highly-trained personnel for sustained operations. In 2010, the Sector's workforce was comprised of approximately 13 million healthcare personnel from many professions, including 5 million first-responders with at least some emergency medical training, 3 million registered nurses, and more than 800,000 physicians. These personnel are vulnerable to attack by terrorists or criminals as well as non-terrorist events such as weather, earthquakes, and epidemics. During such emergencies, the Sector must not only sustain, but also increase its capacity. Today's key issues are safety at the point of care, protection of the workforce, and physical and cyber security, especially given that patient-care organizations have historically designed their facilities to support easy access and customer service rather than workforce protection and surge capacity.

Risks to the Healthcare and Public Health Sector's diverse elements include threats to physical assets, cyber systems, the workforce, and patients. Healthcare facilities are vulnerable to terrorist attacks; to violence against patients and staff; to mishandling of select disease agents or chemical, biological,

[46] For a review and assessment of the U.S. government response to the 2009 H1N1 influenza pandemic, see the June 2011 GAO report, *Influenza Pandemic: Lessons from the H1N1 Pandemic Should Be Incorporated into Future Planning*. Available at: http://www.gao.gov/new.items/d11632.pdf.

pharmaceutical, or radiological materials; and to local and regional events (such as fires, floods, and explosions) that result in an overwhelming surge of patients to healthcare facilities. In addition, the Sector's workforce faces a high likelihood of infection in the course of daily duties. Design guidelines, infrastructure, technology, security controls, personnel training, and operational policies and procedures all influence facility security. Because most assessments and standards focus on only a few of these areas, vast disparities exist across the Sector regarding facility security robustness and effectiveness.

Due to recent legislation such as the Health Insurance Portability and Accountability Act (HIPAA), healthcare organizations have begun to improve information security and workforce and patient safety. Regarding cyber security threats, factors such as lax security in the design of systems and networks have led to web-based vulnerabilities. Cyber threats to date have largely resulted in identity theft, fraud, and data loss. However, more recent events have revealed significant security weaknesses in healthcare systems that can result in the operational failure of medical devices as well as manipulation of systems that now play an increasingly significant role in pharmaceutics, biosurveillance, diagnostics, and direct patient care. Given the proliferation of health information exchanges and recent legislation mandating the adoption of electronic health records (EHRs), cyber threats are likely to increase in importance.

3.0 The Framework and Current State of Intelligence Information Sharing

To account for progress and challenges in intelligence information sharing within the Healthcare and Public Health Sector, fourteen interviews were conducted with subject matter experts representing Sector trade associations and private businesses, including, but not limited to, hospital systems, medical materials manufacturing, health insurance provision, State public health, and mortuary services. Interviews were supplemented by literature review and cross-sector discussion and analysis.

We found that information sharing in the Healthcare and Public Health Sector has a different meaning to small versus large companies, and a different meaning to operations and security personnel versus corporate executives. Historically, private companies have tended to guard and protect their own information due to the many commercial, regulatory, and legal sensitivities surrounding their business interests. With respect to convincing these same companies to engage in information sharing, within the Sector and with the various government agencies concerned, progress is being made through programs of the Sector Coordinating Council (SCC) and various Sector trade associations.

3.1 Framework of Intelligence Information Sharing

At the Federal level, participants in Healthcare and Public Health Sector intelligence information sharing include the Sector Coordinating Council (SCC); the State Department's Overseas Security Advisory Council (OSAC); and the Department of Health and Human Services (HHS), including its office of the Assistant Secretary for Preparedness and Response (ASPR). HHS also serves as the Healthcare and Public Health Sector's Sector-Specific Agency (SSA). At the State level, participants include State trade associations, fusion centers, State Emergency Management Agencies (EMAs), and Homeland Security Advisors. On the local level, participants include regional and metropolitan trade associations, emergency response officials (police, fire, and emergency medical), local public health authorities, local law enforcement agencies, and fusion centers. Internally to the Sector, the Information Sharing Working Group (ISWG) provides intelligence data and other reports to its constituents.

Within the Sector, intelligence information flows from various Federal Government agencies to the leadership of national trade associations; to fusion centers; to local law enforcement agencies; and directly to Sector members through their Homeland Security Information Network (HSIN) portal**.** Staff members who work in emergency preparedness and response for regional, metropolitan, and State-level trade associations may also be receiving briefings from State emergency-management or law-enforcement agencies. Some local public health departments, however, have found that information gets to them slowly and often too late, after it has traveled through their State bureaucracies, and many miss information because their members do not have security clearances. Also, given that suspicious activity and illegal activity are not one and the same, opportunities for obtaining valuable information are frequently missed by Sector entities (e.g., hospitals) due to local law enforcement policies, which prohibit disseminating suspicious activity reports.

Within many large Healthcare and Public Health Sector corporations, intelligence information sharing takes place mainly on two levels: executive and operational. On the executive level, CEOs make decisions, allocate resources, and interface with corporate security personnel. On the operational level, corporate security managers interface with private firms, international partners, State-level entities, and Federal entities in the U.S. Intelligence Community such as DHS, FBI, and DOD. The corporate security managers also interface with facility security managers, who then may have connections to fusion centers, local law enforcement, and trade associations. Hospital systems and healthcare associations tend to have strong internal communication systems such as e-mail alerts, but this internal circulation infrequently extends to sharing beyond company or trade association walls.

Regarding sharing from large corporations to the government, staff may be unlikely to keep watch on a day-to-day basis for information that may be useful to the government. In the event of an incident, hospitals will have much information that is essential for situational awareness on the part of government programs. Yet hospital systems may find they have no clear path for getting information to the government unless it has been specifically solicited, or, having provided information to the government, learning whether any follow-up action was taken. When Sector members do not have an established personal point-of-contact in the agency concerned, requests to government agencies for information often go unanswered.

**Figure HPH-1: Healthcare and Public Health Sector:
Food Safety Scare Incident**

A healthcare system executive received information from the government about a potential food threat, and was able to share it with a food services colleague at Sodexo. Sodexo distributed a nationwide food safety alert, including a list of safety tips and potential threatened areas (e.g., buffet lines). Sodexo's website suggests that information may have circulated as internal bulletins. The company reports: "We provide our managers with convenient access to all current food safety and food security related information through an extensive internal website that contains all new and existing food safety resources, training tools, regulatory updates, information about food security, food emergency planning, food allergies, sanitation and more". Due to internal communication mechanisms within a large healthcare system, good information was shared in a timely manner during this incident.

Source: Sodexo. "Food Safety Facts." 2011.

3.2 Current State of Intelligence Information Sharing

Industry executives and subject matter experts from across the Sector were interviewed to assess the effectiveness of current intelligence information sharing, and also to explore potential ways to improve intelligence information exchanges.

Overall Effectiveness of Intelligence Information Sharing

The sheer size and diversity of the Healthcare and Public Health Sector present obstacles to the effective sharing of intelligence information within the Sector and between the Sector and government. The channels for the flow of intelligence information between the government and the Sector do not seem to be well-known and hence may be underutilized by Sector stakeholders.

Involvement on the Sector SCC was described as greatly valuable for intelligence information sharing. However, beyond participation in the SCC, the “value proposition” for Healthcare and Public Health Sector organizations’ participation in intelligence information sharing and critical infrastructure preparedness activities with government is largely unclear, poor, or absent. Although the Sector is data-rich, members do not clearly understand the value of their potential contributions to the nation’s overall infrastructure protection and intelligence effort, and it is unclear whether sharing with government directly generates follow-up or other security benefits for organizations that would consider sharing. In addition, providing information to the government is poor due to lack of mechanisms, inadequate knowledge of mechanisms that do exist, and fear of legal and regulatory risks. Information sharing between Sector organizations is poor due to business competition risks.

Generally, intelligence information provided by the Federal Government to members of the Healthcare and Public Health Sector is considered reliable, but it does not provide useful and sufficient intelligence information to the right recipients in a timely manner. Intelligence analysts not intimately familiar with healthcare and public health may not know about the important interdependencies between the Healthcare and Public Health Sector and the other sectors. Also, the uniqueness of a State’s regulatory context may make the applicability of Federal Government information problematic, and the intelligence information the government makes available during an incident may also have been provided through other sources in a more timely fashion. Accordingly, to improve both relevance and timeliness, Sector members often purchase this information from private companies or attain it from openly available public sources.

Information provided by government programs such as the Center for Disease Control (CDC) and the HHS Assistant Secretary for Preparedness and Response (ASPR) is seen as improving with time, with decreased redundancy and increased relevance. However, styles of engagement between Federal and local partners vary by incident; roles and responsibilities for information collection and sharing seem unclear and potentially duplicative across agencies; follow-up on the part of government entities is often poor; and the national system for providing security clearances for private-sector personnel to obtain intelligence information remains highly complicated and confusing.

Figure HPH-2: Healthcare and Public Health Sector: Anthrax Letters Scare

In the months following September 11th, public fears focused on the possibility of terrorist use of “dirty bombs” and anthrax letters. Letters containing anthrax spores had been mailed to news media personnel and congressional officials in the fall of 2001, leading to the first cases of anthrax infection related to an intentional release of anthrax in the United States. The American Hospital Association initially received vague information, which was only enough to cause worry and to tell the hospitals that they should be planning and communicating with each other if a threat occurred. Better, more locally-relevant information might have been available through local agencies and law enforcement. Local and State public health officials in the epicenters of the anthrax incidents reported that communication among response agencies was generally effective, but public health officials had difficulty reaching clinicians to provide them with guidance.

Source: Government Accountability Office. Public Health Response to Anthrax Incidents of 2001. 2003.

Within the Sector, hospitals are reluctant to share intelligence information with competing businesses or with authorities who provide regulatory oversight for fear of legal and business risks. In addition, suspicious-activity information of interest to hospitals may not be the same as unlawful activity of interest to law enforcement. In general, fusion centers and local law enforcement agencies are not well-connected to members of the Healthcare and Public Health Sector nor conversant in the Sector’s intelligence information requirements.

Other challenges that have arisen in communicating intelligence information between the government and the Sector include: responsibility for emergency management and response is not always a full-time assignment for corporate personnel; the meaning of “critical infrastructure protection” is unclear to many Healthcare and Public Health Sector members; getting significant participation from high-level corporate executives poses a challenge; and there is an ongoing risk of the inadvertent release of competitive data.

How Intelligence Information Sharing Works in the Healthcare and Public Health Sector

Members of the Healthcare and Public Health Sector derive the intelligence data they do obtain, both classified and open-source, from all types of sources: government, private sector, internal corporate sources, commercial intelligence reporting services, fusion centers, local law enforcement agencies, and industry trade associations.

Intelligence information sharing is driven by mechanisms such as public policy, available technology, working groups, and other convening bodies. Private companies in the Sector regularly use nongovernment resources such as paid intelligence providers. Newspapers and other open-source reports have particular value to elements of the Sector which are geographically fixed and need intelligence information on potential threats restricted to their own area. Hospitals have local and regional planning meetings to address security concerns and can often acquire intelligence information regarding suspicious activities or threats from each other.

To the extent that relevant information circulates internally to the affected community, today’s Healthcare and Public Health Sector is characterized by a significant level of “horizontal” information sharing that does not rely directly or primarily on government entities. Businesses and other participants in the Sector spontaneously organized into groups and associations with common interests in discussing intelligence information and security issues; examples include the Asset Protection Executives (APEX) and a similar group called the Industrial Security Management Association (ISMA).

Healthcare and Public Health Sector Intelligence and Information Requirements

Intelligence information required by the Healthcare and Public Health Sector plays two main roles: enabling the protection and resilience of Sector assets, and enabling effective biosurveillance. In the context of human health, biosurveillance is defined by the Department of Health and Human Services as the science and practice of managing health-related data and information for early warning of health threats and hazards, early detection of related events, and rapid characterization of the event so that effective actions can be taken to mitigate adverse health effects. As such, the Healthcare and Public Health Sector needs to receive intelligence information on any issue that has the potential to have a health impact on communities or specific individuals therein. To date, much attention has been focused on biosurveillance (a traditional public health function) and data protection (a legal requirement), but less attention has been focused on infrastructure protection.

Local public health leaders require information on any issue that could pose a public health threat—whether a spill of hazardous materials, an explosion, the spreading or introduction of chemicals or other biological agents, a mass fatality event that could overwhelm funeral directors, or any other health hazard. Also, local public health officials need awareness of activities located within their geographic area that involve threats of potential toxicity.

Hospital systems, and other large geographically-fixed organizations and networks, require information on threats (e.g., natural disasters, criminal incidents, crashes, and weather-related disasters) that are likely to affect healthcare providers by causing spikes in demand and/or specialized medical needs. For intelligence purposes, these facilities use internal-system monitoring as well as information from government agencies, local law enforcement agencies, and the local business community. Geographically-fixed entities also tend to closely monitor open-source news reports in their local area.

Although it is commonly assumed that hospitals will be able to scale their services to address a surge in patients, they need approximately four days' advance notice to be assured that they can provide the services needed. Hospitals benefit from having multiple sources of intelligence information which enables them to synthesize what is important given the nature of the threat and the location of the facilities. During a crisis, hospitals also benefit from receiving information which they can then communicate to the public.

The prevalence of small businesses within the Sector is a major concern. Compared to larger companies, small businesses are not able to move resources between facilities, and therefore are especially reliant on advanced news of potential threats. The majority of hospitals nationwide, for example, have less than 100 beds, and the subsector providing mortuary services is almost entirely comprised of family-owned businesses. Information from industry trade associations is particularly important for these smaller organizations, but even their own trade associations cannot reach each and every business of the type they represent.

Figure HPH-3: Healthcare and Public Health Sector:
False Hospital inspectors

Individuals with identification from the Joint Commission arrived at hospitals in several states, posing as inspectors and surveyors. They were identified as imitation inspectors who were targeting hospitals in Los Angeles, Boston, Detroit, Indianapolis, and elsewhere. Either DHS or the FBI had information about this fraud, and DHS warned the national hospital association (the AHA) with an Information Bulletin alert on April 25, 2005. The bulletin was intended to raise awareness about the suspicious activity. The AHA shared the intelligence information with State hospital associations, which resulted in associations disseminating advisories, directing hospitals to inform security and front-desk teams. However, the alert bulletin originally received by the AHA was marked FOUO; and after sharing the information with State associations, the AHA was mildly reprimanded. This event demonstrated that there was a lack of clarity on how to use FOUO information.

Source: U.S. Department of Homeland Security. False Hospital Inspectors. 2005.

SCC members of the Healthcare and Public Health Sector require and value threat information, both general and specific, to inform preparedness efforts, as well as information on best practices in threat mitigation. They cite the importance of developing relevant information drawn from classified and For Official Use Only (FOUO) sources so that it can be shared with a broader audience. Even the FOUO designation, however, may provoke confusion over appropriate use of that information.

4.0 Findings

Four findings best summarize the status of intelligence information sharing from the perspective of the Healthcare and Public Health Sector.

Finding 1: Healthcare and Public Health

Sources and mechanisms: Currently, there is no formal set of mechanisms for intelligence information-sharing within the Sector, and there is room to improve existing mechanisms for sharing between local facilities and Federal agencies.

- Healthcare and Public Health Sector members have never established an internal culture of intelligence information sharing, and are not currently engaged in substantial two-way sharing with the Federal Government. Regarding communication with Federal agencies, Sector members such as local public health departments are finding that information only gets to them slowly after it travels through State bureaucracies. And many Sector members miss opportunities to get information because they do not have security clearances or the right personal contacts. Fusion centers are poorly connected to Sector members in general and hospitals in particular. In this context, SCC participation does remain valuable in tying Sector members to Federal contacts in the U.S. Intelligence Community. HSIN, the web portal used by DHS and HHS to share sensitive but unclassified (SBU) information with their trusted partners, has also made some progress in connecting local users to Federal intelligence information. However, it currently requires multiple logons, which expire on a regular basis. This poses a challenge for intermittent users, who can find themselves locked out; access frustrations threaten to decrease some Sector members' use of the portal.

- Sector members are interested in more mechanisms to get intelligence information from the government to the private sector. HHS, which has an internal intelligence-sharing function that is well-tied into the U.S. Intelligence Community, could share externally their daily internal briefing on the state of the nation in public health. This would benefit public health leaders on many levels. Testing the flow of intelligence information between fusion centers and hospitals, and testing of other notification mechanisms, should be conducted regularly to ensure that hospitals and other Sector members receive required intelligence information on a timely basis.
- Insufficient mechanisms exist for the private sector to provide intelligence information to the Federal Government. Sector members would also value more feedback on how the government uses the intelligence information it does receive from them. This would build trust by demonstrating that the effort expended in reporting to and communicating with the Federal Government creates benefit, and would motivate further response.

Finding 2: Healthcare and Public Health

Participants: Intelligence information sharing in the Healthcare and Public Health Sector is now largely dependent on an individual's choice to share information through use of existing mechanisms; on personal relationships with key contacts; and on memberships in trade associations.

- Individuals are the key for making use of existing mechanisms and taking opportunities to participate in intelligence information sharing. There is a need for greater participation in the use of existing mechanisms, such as HSIN, by the broad Sector membership. Training and other outreach programs need to be developed and actively pursued.
- Personal relationships remain important. Executives of Sector organizations may have Federal agency contacts from activities they have participated in or from previous positions held within those agencies. Sector members without such contacts frequently wish to develop them. However, the high rate of personnel turnover in Federal jobs serves as a barrier to maintaining these trusted relationships.
- Trade associations are particularly important for promoting information sharing within diverse sectors and within those sectors with a large presence of small businesses. Challenges experienced by the Healthcare and Public Health Sector in receiving and transmitting intelligence information relate to both the number and size of organizations (i.e., either so large that information may not reach the right decision maker or so small that the organization may be overlooked entirely). In this context, trade associations are particularly valuable mechanisms to distribute intelligence information received from the Federal Government and to forward inquiries and incident reports to Federal agency points of contact.

Finding 3: Healthcare and Public Health

Collaborative relationships: There is a need for greater integration of the Healthcare and Public Health Sector with local law enforcement agencies, fire departments, and emergency service providers, as well as with fusion centers.

- Other sectors, governments, and law enforcement agencies need to think of the Healthcare and Public Health Sector as interdependent and, therefore, include them in emergency response preparations and intelligence information sharing. Some Sector members doubt whether the government will inform them of relevant threat intelligence. Vague or general information about threats that reaches hospitals may possibly cause more anxiety than it resolves. It implies that the government has some intelligence about a threat, yet cannot share the actual message. Government intelligence information provided to hospitals is often seen as old, and leaders of companies producing medical materials and pharmaceuticals, for example, have come to rely on private companies for intelligence. It is essential to raise the visibility and increase the perceived importance of the Healthcare and Public Health Sector as essential critical infrastructure to inform, protect, and include in preparedness efforts.
- Increased collaboration is needed between fusion centers and other participants beyond local law enforcement agencies; i.e., the Healthcare and Public Health Sector, other critical infrastructure, and the U.S. Intelligence Community. Although the Federal Government works well with State public health departments, it is challenging to get local public health departments to participate in fusion centers. There is a need to ensure that intelligence information transmitted from DHS to fusion centers is then transmitted from fusion centers to State health departments, local governments, and private-sector members of the Healthcare and Public Health Sector. Local healthcare providers and fusion center representatives need to have more knowledge and awareness of what each does and what each needs to know. Both fusion centers and local law enforcement agencies should conduct increased outreach to hospitals and other Sector organizations.
- There is a need for more exercises and drills that bring together healthcare providers and first responders. Exercises and drills offer trust and relationship-building benefits as well as actual practice in disaster response. Bringing fusion center personnel together with local health care personnel more often in both larger and smaller venues would help build these important relationships. Increased sponsorship of multi-agency drills is recommended.

Finding 4: Healthcare and Public Health

Security classifications: Healthcare and Public Health Sector members would benefit from greater access to sensitive information, from better guidance on how to handle FOUO information, and from information that has been analyzed and provided in more actionable forms.

- Classified briefings offered the Healthcare and Public Health Sector have a mixed audience, and participants have particularly valued the opportunity to discuss issues with each other on the classified level. The private-sector has worked effectively through DHS to obtain security clearances for its employees, but the State-level participants have had a harder time; hence there is a new program in place to obtain clearances for State-level personnel through HHS. Greater support also should be made available for obtaining security clearances for local health department personnel. It is not advisable, however, to address the challenge of distributing sensitive intelligence information solely through increasing the number of cleared individuals and classified briefings. Given that a great deal of information relevant to the Sector is protected under the Health Insurance Portability and Accountability Act (HIPAA), Sector members have experience in handling protected information. The government should place greater trust in the

Sector's ability to handle and manage sensitive information, and should make a concerted effort to develop and distribute more unclassified intelligence.

- There is a need for better guidance on how to handle FOUO information. Both the government and the private-sector have participants who are unclear on how to share FOUO information and with whom to share it. This lack of clarity has the potential to slow intelligence information sharing, particularly during critical incidents.
- Intelligence information provided by the government to the Healthcare and Public Health Sector can be too broad and insufficiently actionable for front-line emergency responders. Busy executives need intelligence information that has been analyzed to show trends and implications. One local public-health leader requested an executive-level report on a periodic basis, probably about every 4-5 days, highlighting trends, synthesizing them into specific threat risks, and clearly stating whether events being described are old or new events. More specifically, public-health leaders need information to help them decide when to remove resources and focus from one specific type of threat, and employ them on another type of threat instead. With threats ranging from terrorist assaults to dirty bombs, facilities need to know where the greatest risks fall at a given point in time. To help meet this need, HHS could announce the point in time after which they are recommending scaling back the amount of attention being paid to a specific threat.

5.0 Conclusions

The members of the Healthcare and Public Health Sector Case Study believe the following four conclusions are of the highest priority to the Sector at this time:

Conclusion 1: Healthcare and Public Health

DHS and the Healthcare and Public Health Sector SCC and Government Coordinating Council (GCC) should support educational efforts on the Sector's role in information sharing and an increased number of multi-agency drills for potential incidents affecting Sector facilities.

- The Healthcare and Public Health SCC and GCC should develop, with support from the CDC and DHS PPIS, a series of educational presentations to distribute to SCC members to inform their organizations of the important roles played by the Sector in achieving national critical infrastructure protection and resiliency goals. A significant portion of the Sector may not fully understand their role in the nation's preparedness, protection, and resilience strategies.
- DHS should incorporate Healthcare and Public Health multi-agency exercises into existing critical infrastructure and key resources (CIKR) exercise programs and existing national-level exercises. Multi-agency drills will raise awareness among Healthcare and Public Health Sector participants, local law enforcement agencies, fusion centers, and local public health authorities of the types of roles that each may play in a hypothetical threat incident. Drills will also serve to build trusted relationships, strengthen intelligence information sharing, broaden sector involvement in national and regional planning, and raise the visibility of healthcare organizations as participants who need to receive intelligence information.

Conclusion 2: Healthcare and Public Health

DHS and Sector members should improve their understanding of existing information-sharing mechanisms.

- The Healthcare and Public Health Sector SCC and GCC should establish a Working Group under the auspices of CIPAC to identify the Sector's priority requirements for intelligence. A Working

Group could start by assessing information sharing associated with the previous pandemic influenza preparedness efforts and Sector needs to respond effectively to mass casualty events associated with the National Planning Scenarios.

- The CDC, DHS, and the Office of the Director of National Intelligence (ODNI) should collaborate to create an Information Flow Map to graphically link sender, recipient, application, and other details to enable the Sector to better understand existing intelligence-information networks. Because of the complexity of this task, it is suggested that limited models first be created based on the known intelligence requirements of key critical infrastructure members of the Sector.
- The DHS Office of Intelligence and Analysis (I&A) should increase the level of Healthcare and Public Health Sector expertise represented by its Sector Specialists.

Conclusion 3: Healthcare and Public Health

Trade associations in the Healthcare and Public Health Sector should be used as one of multiple channels for information sharing.

- DHS should promote the inclusion of Healthcare and Public Health Sector trade associations in intelligence information-sharing efforts. While getting information through established chains of command, such as from the Federal Government to the national trade association to State and local trade associations, allows for development of trusted relationships, but it is also slow and tends to restrict information flow. While trade associations and their national, State, and local hierarchy are a valuable mechanism for bidirectional information flow, they should be accompanied by other mechanisms for direct sharing between Federal and local participants.
- Healthcare and Public Health Sector trade associations should designate information-sharing specialists as liaisons to DHS and other members of the U.S. Intelligence Community. This would establish or reinforce mechanisms to get information from their organizations to the U.S. Intelligence Community.
- HSIN's administrators should establish a single logon for each user rather than multiple logins to multiple communities. Given that in many small companies and local public health departments, a single professional may serve in security/preparedness as well as other roles, it is essential that mechanisms for sharing information support a multi-tasking schedule. A single logon to HSIN, giving access to multiple communities, could help resolve the fact that multiple logons expire too frequently for HSIN to be a useful tool for local private or public-sector employees who only check the site intermittently or when prompted by awareness that new-event information may be available.
- Mechanisms should be tested regularly to ensure that they are able to transmit information to Sector members.

Conclusion 4: Healthcare and Public Health

DHS should further distribute clear guidance on how to handle FOUO information; in parallel, they and members of the U.S. Intelligence Community should increase the distribution of unclassified versions of the material.

- The U.S. Intelligence Community should develop tear-line versions of intelligence information documents for Sector partners. It is essential that intelligence information sharing not be hindered by uncertainty on how to handle FOUO information—both for initial distribution to Sector members and for their later redistribution and communication. Sector members are accustomed to dealing with private and sensitive information, such as through HIPAA, and have shown that they are able to be trusted.

Appendix F. Case Study: Oil and Natural Gas Sector

TABLE OF CONTENTS

1.0 Introduction

The Oil and Natural Gas (ONG) Sector has adopted an all-hazards approach to risk management, encompassing natural events, criminal acts, insider threats, and foreign and domestic terrorism. The sector closely monitors risks associated with global events and foreign operations; physical and cyber facilities, networks, and control systems; insider threats; interdependencies; and terrorism. The sector also is very concerned with maintaining public and investor confidence. The sector places considerable focus on restoration as a cornerstone of business continuity and continuous operations.

To meet these evolving security challenges, intelligence and information sharing within the ONG Sector has significantly improved in the past few years. Both the sector and the Federal Government have moved from reluctance to share information to a culture of wanting to exchange useful, credible, and timely information. At the same time, however, there remains within the sector a concern over the protection of information voluntarily shared with the Federal Government.

While the ONG Sector can determine risks, consequences, and vulnerabilities on its own, the sector relies on the Federal Government and local law enforcement to relay useful threat information in a timely manner. Of special importance to the sector is information on potential attacker motivation, likely targets, and probable mode of attack. General threat information is not as useful to the sector as information that can inform sector risk-management strategies and facility protective measures.

2.0 Sector Profile

As a subsector of the Nation's Energy Sector, the Oil and Natural Gas (ONG) Sector includes the production, refining, storage, and distribution of oil and gas.[47] The ONG Sector supplied nearly 65 percent of U.S. energy needs in 2008, with facilities and pipelines distributed across the entire country.[48] (See Figure ONG-1 for a summary of key ONG assets in the United States.) Virtually all sectors of the economy depend on the ONG Sector for their power needs, and the ONG Sector itself is dependent upon the Transportation, Information Technology, Communications, Banking and Finance, and Government Facilities Sectors. The ONG Sector also operates closely with the petrochemical industry. ONG has a large international presence: in 2008, some 60 percent of the crude oil required by the United States was imported, and nearly 13 percent of its liquefied natural gas consumption came from overseas suppliers.[49]

The petroleum portion of the ONG Sector includes the production, transportation, and storage of crude oil; processing of crude oil into petroleum products; transmission, distribution, and storage of petroleum products; and sophisticated control systems to coordinate storage and transportation. The natural gas portion includes the production, processing, transportation, distribution, and storage of natural gas;

[47] For a discussion of the electric power subsector of the Energy Sector, see National Infrastructure Advisory Council, *A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council* (Washington, DC: NIAC, October 19, 2010), http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf. The terms "ONG subsector" and "ONG Sector" are used interchangeably in this case study report.

[48] The following description of the ONG Sector primarily uses the following sources: Department of Homeland Security and Department of Energy, *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan* (Washington, D.C.: DHS, 2010), http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf; and DHS webpage on "National Infrastructure Protection Plan: Energy Sector Snapshot," http://www.dhs.gov/xlibrary/assets/nipp_snapshot_energy.pdf.

[49] For a discussion of the growing role of natural gas to the U.S. economy and its implications, see CRS, *Global Natural Gas: A Growing Resource* (R41543, December 2, 2010), http://www.fas.org/sgp/crs/misc/R41543.pdf.

Figure ONG-1: Oil and Natural Gas Sector: Key Facts

Petroleum

Petroleum supplied 37 percent of the total energy consumed in the United States in 2008.

Key petroleum products: Motor gasoline, jet fuel, distillate fuel oil, residual fuel oil, and liquefied petroleum gases.

Production assets: In the United States, there are 525,000 crude oil-producing wells, 30,000 miles of gathering pipeline, and 51,000 miles of crude oil pipeline.

Refineries: In the United States, there are 150 operable petroleum refineries, 116,000 miles of product pipeline, and 1,400 petroleum terminals.

Control systems: Petroleum relies on sophisticated supervisory control and data acquisition (SCADA) and other cyber systems to control production, distribution, and monitoring.

Storage: Crude oil and petroleum products are stored in tank farms and other facilities.

Imports: Both crude oil and petroleum products are imported, primarily by ship. In 2008, some 66 percent of the crude oil required to fuel the U.S. economy was imported.

Natural Gas

Natural gas supplied 24 percent of the total energy consumed in the United States in 2008.

Production assets: In the United States, there are more than 478,500 gas production and condensate wells and 20,200 miles of gathering pipeline.

Processing: In the United States, gas is processed at more than 550 operable gas processing plants and there are almost 300,000 miles of interstate pipeline for the transmission of natural gas.

Control systems: Centralized gas control stations collect, assimilate, and manage data received from compressor stations all along the pipeline. These control systems can integrate gas flow and measurement data with other accounting, billing, and contract systems.

Storage: Gas is stored at 399 underground storage fields and 103 liquefied natural gas (LNG) peaking facilities.

Distribution: Natural gas is distributed to homes and businesses over 1,200,000 miles of intrastate distribution pipelines.

Imports: Imports of LNG are increasing to meet growing demand. In 2008, some 12.7 percent of total U.S. LNG consumption was imported.

Sources: Energy Sector 2010 SSP; DHS NIPP Snapshot: Energy Sector; CIPAC Annual. Figures are mostly 2008 figures.

liquefied natural gas (LNG) facilities; and gas control systems. The petroleum and natural gas segments of the Energy Sector are integrated into the ONG Sector Coordinating Council (SCC), separate from the Electricity SCC, established to coordinate the infrastructure protection activities of the owners and operators of these critical infrastructure as prescribed by the National Infrastructure Protection Plan (NIPP).

The ONG Sector is characterized by diverse assets, systems, and networks, as well as wide geographic dispersion. Because of its complexity and geographic expanse, the sector is constantly exposed to a wide variety of risks to physical plants and associated human and cyber systems.[50]

In terms of natural hazards, hurricanes are the most frequent type of threat to the ONG Sector, due to the location of many refineries in coastal areas. Hurricanes often cause the preemptive shutdown of facilities, even if the facilities themselves are not directly affected by the storm. Through years of experience in preparing for and responding to hurricanes, the ONG Sector has significantly reduced its vulnerability and increased the overall resilience of its product supply chain through such measures as

[50] For an overview of critical infrastructure protection efforts in the ONG Sector, see *The CIP Report*, Vol. 9, No. 9 (March 2011), which featured the sector. Available at: https://www-gs.llnl.gov/data/assets/docs/publications/2011-mar24_issue104_oil-gas.pdf.

building in redundancy of operations, dispersion of assets, and the ability to adjust to and compensate for lost assets. One of the sector's continuous security goals is to harden its infrastructure to better prepare for hurricanes and other natural disasters.

The sector has strong risk-management programs in place or under development to improve security and resilience. Current ONG security programs focus on global threats, physical threats, cyber security, methods used by terrorists and criminals, and improvements in processes such as intelligence and information exchange. Efforts to improve public-private information sharing within the ONG Sector include such activities as developing protocols and tools for secure data exchange and communications, ensuring legislative bodies understand the need to protect sector-specific critical assets and sensitive sector information, expediting security clearances, and strengthening environments for securely sharing U.S. government information on threats with asset owners and operators.

3.0 Oil and Gas Natural Information Sharing Framework and Processes

The ONG Case Study Group conducted interviews with industry executives and subject matter experts from across the sector to assess the effectiveness "on the ground" of current intelligence information sharing between the sector and government at all levels. This section discusses the framework of intelligence information sharing relationships in the ONG Sector and the sector-specific information needs. The next section assesses the effectiveness of the mechanisms and processes for sharing threat and intelligence information in the sector. Sections 4 and 5 of this case study detail the Case Study Team's findings based on these interviews and associated recommendations.

3.1 Information Sharing Relationships in the Oil and Natural Gas Sector

The exchange of intelligence information within the ONG Sector occurs at many different levels, including the ONG SCC and its various working groups, programs with DHS, and relationships with regulatory agencies such as the Department of Energy (DOE) and the Department of Transportation.

ONG Sector Coordinating Council

The ONG SCC is a vital information-sharing mechanism within the sector because its members represent more than 98 percent of ONG owners and operators. The SCC was formed by ONG owners, operators, and trade associations and serves as a broad industry-wide network to help coordinate industry initiatives and partnerships with government. It is important to note that many of the trade associations have very active security committees, which provide a forum for the exchange of threat information to their various members.

The ONG SCC participates in a number of joint SCC and GCC working groups functioning under the Critical Infrastructure Partnership Advisory Council (CIPAC) to address specific subjects of concern to sector members. The ONG SCC also is developing performance metrics based in part on the Chemical Sector's voluntary metrics program. Alignment between these two groups is important because many oil and natural gas companies' assets are related to the Chemical Sector.

Department of Homeland Security

The DHS Office of Infrastructure Protection (DHS IP) coordinates periodic and routine updates concerning threats to the ONG Sector. The threat updates are provided to vetted and/or cleared members of the ONG SCC and their member companies. Threat updates at the For Official Use Only (FOUO) level are provided monthly through teleconferences that convey global and domestic physical and cyber threats to sector members. The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) provides the physical threat updates, and the DHS National Cyber Security Division's (NCSD)

Industrial Control System-Computer Emergency Readiness Team (ICS-CERT) provides updates for cyber threats.

DHS also disseminates periodic written products. Products on physical threats include Homeland Security Notes, Homeland Security Assessments, and Homeland Security Reference Aids that are posted to the Homeland Security Information Network – Critical Sectors (HSIN-CS) and the ONG Sector portal (HSIN – ONG) on that network. Daily, weekly, and monthly cyber-threat updates are issued in the form of FOUO Critical Infrastructure Information Notices and Homeland Security Cyber Security Monitor Issues. Members of the ONG SCC who wish to receive instant notification of cyber threats can gain access to the Energy portal on the secure ICS-CERT website.

DHS IP also coordinates classified threat briefings for cleared members of the ONG Sector. To broaden the participation in these classified threat updates, DHS IP sponsors security clearances for members of the ONG SCC who are employees of oil and natural gas companies and associations with a need for threat information. A variety of agencies, including DHS HITRAC, the Transportation Security Administration (TSA), the Federal Bureau of Investigation (FBI), DOE, and other members of the U.S. Intelligence Community, provide briefings at these semi-annual events.

The Pipeline Security Division of TSA enhances the security preparedness of the Nation's hazardous liquid and natural gas pipeline systems.[51] TSA also provides pipeline security stakeholder conference calls to share and exchange information, to educate industry on new security initiatives and programs, and to give industry an opportunity to ask questions and bring up security issues for discussion.

Another mechanism that works to improve information and intelligence flows between the ONG Sector and government is the DHS NPPD/IP Protective Security Advisors (PSA) program. PSAs coordinate vulnerability assessments within their region and serve as pre-designated infrastructure liaisons at Joint Field Offices during contingency events. A related and newer program that has strong potential to enhance communications between the ONG industry and DHS is the Regional Resiliency Assessment Program (RRAP), which coordinates interagency resilience analyses of critical infrastructure on a regional level.

Department of Energy

Within DOE, the Office of Electricity Delivery and Energy Reliability has been assigned the role and responsibilities of the Energy Sector-Specific Agency (SSA). DOE, in consultation with its security partners, has established sector goals, one of which is to "establish robust situational awareness within the sector through timely, reliable, and secure information exchange among trusted public and private sector partners."[52]

Publically available information about the ONG Sector is provided by the DOE Office of Infrastructure Security and Energy Restoration (ISER). Periodic reports issued by this office include the Energy Assurance Daily, Emergency Situation Reports, and Analysis and Outreach Reports. ISER is responsible for applying DOE's technical expertise to ensure the security, resilience, and survivability of key energy assets and critical energy infrastructure at home and abroad. ISER works closely with DHS, the Federal Energy Regulatory Commission (FERC), and other National, regional, State, and local governments and commercial organizations to support the National critical infrastructure protection program; analyze

[51] See http://www.tsa.gov/what_we_do/tsnm/pipeline.shtm.

[52] Energy SSP, p. 1.

infrastructure vulnerabilities and recommend preventive measures; and develop, implement, and maintain a National energy cyber security program.

DOE also works under CIPAC to interact with government stakeholders and representatives of ONG owners and operators. In addition, DOE collaborates with the sector's use of HSIN-CS. HSIN – ONG provides mechanisms by which the ONG industry can share and analyze important information about vulnerabilities, threats, intrusions, and anomalies, and through which it can communicate with and provide support to the Federal Government. Also, DOE's secure ISERnet website contains the Energy Industry Assurance Coordinators (EIAC) system, a database of key industry personnel who can exchange information with DOE during energy emergencies. The site provides threat awareness and relevant security analyses and presentations.

Control systems are an issue of major concern to DOE, and the 2006 *Roadmap to Secure Control Systems in the Energy Sector* and updated 2011 *Roadmap to Achieve Energy Delivery Systems Cybersecurity* identify steps to secure ONG control systems over 10 years.[53] Information sharing between the government and private sector was identified as a key component of developing and disseminating solutions to cyber vulnerabilities as these become known.

Department of Transportation and Other Federal Agencies

The Department of Transportation (DOT) is the SSA for all pipelines in the United States, including those carrying petroleum products and natural gas.[54] ONG relies on pipelines, barges, tankers, railways, and highways to transport its raw and refined products. DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) coordinates activities regarding oil and natural gas pipelines, and is a member of the interagency committee charged with facilitating prompt repair of oil and natural gas transmission pipelines. DOT's Maritime Administration (MARAD) programs promote the use of waterborne transportation and its integration with other segments of the transportation system. MARAD also supports the ONG Sector by ensuring reserve shipping capacity in times of National emergency.

The ONG Sector also interacts with several other regulatory Federal departments and agencies, including the Department of the Interior (especially the Minerals Management Service, which manages the Nation's natural gas and oil resources on the Outer Continental Shelf), the Department of State (which is involved with ONG overseas operations and international agreements), the Environmental Protection Agency (responsible for air quality and fuel-related emissions), and the National Oceanic and Atmospheric Administration (which oversees environmental damage assessments in coastal waters). Another important regulatory regime governing parts of the ONG Sector is the Maritime Transportation Security Act (MTSA), administered by the U.S. Coast Guard. MTSA has several requirements for offshore ONG facilities in regards to vulnerability assessments, information sharing, and reporting.[55]

State and Local Governments

State and local governments are critical in providing a secure and reliable ONG infrastructure for the Nation. Their agencies are responsible for emergency planning and response, developing energy security and reliability policies and practices, and facilitating ONG Sector protection activities. Of special

[53] See www.controlsystemsroadmap.net.

[54] For information related to pipeline security, see GAO, *Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes* (GAO-10-867, August 2010), http://www.gao.gov/new.items/d10867.pdf; and CRS, Keeping America's Pipelines Safe and Secure: Key Issues for Congress (R41536, March 17, 2011), http://www.fas.org/sgp/crs/homesec/R41536.pdf.

[55] See http://www.ilta.org/LegislativeandRegulatory/MTSA/MTSAinfo.htm.

importance are State government energy offices, represented by the National Association of State Energy Officials (NASEO). These offices coordinate responses to energy emergencies, develop emergency plans, and develop practices to improve energy security and reliability.

State public utility commissions, represented by the National Association of Regulatory Utility Commissioners (NARUC), play a critical role in regulating utilities at the State level. The commissions are involved in cost-recovery issues, energy-supply curtailment plans, emergency response, cyber security, and critical infrastructure protection (CIP) activities. NARUC's Critical Infrastructure Committee is the focal point for this effort.

Governors' offices and State legislators, represented by the National Governors Association (NGA) and the National Conference of State Legislatures (NCSL), respectively, assist State and local governments in developing policies that affect ONG Sector security and play major roles in responding to energy emergencies. These State-level decision makers coordinate with Federal and industry groups on ONG security and emergency issues, and possess emergency authorities they may exercise to mitigate the impacts of crises in the ONG Sector. Governors are assisted by State Homeland Security Advisors, which coordinate and conduct homeland security activities at the State level, including programs involving ONG infrastructure protection and vulnerability analysis.

On the front lines of emergency response at the State and local levels are State and local emergency management agencies, represented by the National Emergency Management Association (NEMA) and the International Association of Emergency Managers (IAEM). These first responders prepare for and respond to all emergencies, including those with implications for ONG infrastructure.

Local governments and associations that represent them, such as the Public Technology Institute (PTI), comprise an extremely large set of stakeholders. Many local governments with ONG facilities located in their jurisdictions play an essential role in ONG Sector security, protection, and emergency preparedness.

At the National level, the Energy Emergency Assurance Coordinators (EEAC) system is a cooperative effort among NASEO, NARUC, NCSL, NGA's Center for Best Practices, PTI, and DOE's ISER. The system establishes a secure cooperative communications environment for State and local government personnel with access to information on energy supply, demand, pricing, and infrastructure. Designated members have expertise in electricity, petroleum, and natural gas. The EEAC system is housed on DOE's ISERnet website.

3.2 Information Requirements to Meet Security Responsibilities

We found that of the various kinds of intelligence made available from the government, the most valuable to the ONG Sector was threat information. Depending upon the nature of the company's business model, threat information could focus on domestic terrorism, international terrorism, insider threats, or even criminal threats. Mostly, those interviewed expressed a need for threat information that was both specific and credible, rather than more general.

From the interviews, it appeared that some companies—particularly the smaller ones—had fewer threat concerns than larger companies with a higher risk profile. Larger companies with an international presence often had excellent relationships with the State Department's Overseas Security Advisory Council (OSAC), the U.S. intelligence community, and foreign security agencies in the countries/regions within which they operated.

The ONG Sector would like to receive more FOUO information that would allow for greater access across the sector to personnel without clearances. The sector does not need access to information related to ongoing investigations, but it would like to know information that might enable ONG security specialists to conduct their own analysis of potential impacts to their facilities or operations.

In recent years, the ONG Sector has worked closely with the DHS Office of Intelligence and Analysis (I&A) to develop Sector Intelligence Needs (SINs). An “ONG playbook” is being drafted that includes specific sector information/intelligence sharing needs, but uncertainty remains as to when this document would be published.

Those interviewed reported very helpful information coming out of sector participation in exercises with the Federal Government. Especially noteworthy were Red Team/Blue Team exercises on supervisory control and data acquisition (SCADA) systems sponsored by DOE. Also, reviews of control systems by US-CERT were well received.

There seemed to be consensus in the interviews that the ONG Sector and DHS needed to continue to work closely to better refine the type of information actually needed by the sector. General threat information was less useful than information concerning, for example, how a specific pipeline was attacked and what methods were used. The sector would like access to case studies to learn what is happening elsewhere in the world (e.g., refinery bombings) in order to apply the lessons learned to U.S. facilities or operations.

All of those interviewed indicated that the timeliness of government-provided intelligence and information is an issue. The industry works in a 24/7 environment, so information arriving late is of little use. For FOUO alerts, for example, the immediacy often has already passed. Interviewees reported that the government vetting process has so many layers that it negatively affects the timeliness of information received by the sector. Often, the DHS/FBI/USCG documents are programmatically helpful but not helpful in an operational sense. For these reasons, security officers in corporations often use the government information merely as a verification of what they have already found from other sources and news media.

It was apparent from the interviews that ONG companies look to all sources for threat information. Government intelligence is only one source, but it can play a very important role, if the threat information is packaged to meet the needs of the recipient companies.

In terms of cyber security, we heard that valuable information from government could relate to operating systems (e.g., XP-7, Server 2000, Unix) that SCADA systems rely on. The sector wants to know about the vulnerabilities in its hardware. A survey would be helpful on what type of equipment companies use so that the government could provide tailored intelligence on specific vulnerabilities. This kind of information is now mostly received through vendors. Also of use would be information on where common problems have appeared, such as phishing attempts or smart-phone viruses.

4.0 Effectiveness of Information Sharing in the Oil and Natural Gas Sector

In general, interviewees reported that intelligence information sharing between the ONG Sector and the Federal Government has improved significantly since the September 11 attacks. The sector draws a clear distinction between “intelligence” and “information,” with intelligence being information that has been analyzed. An ONG Intelligence Requirements Working Group has been working with DHS to improve the quality of information so that resulting intelligence can be more useful; that is, credible and actionable.

The Working Group has worked closely with the ONG Sector Specialist at DHS to provide the absolute maximum information without divulging classified information.

Threat information provided by the Federal Government has become much more helpful and valuable. However, some of the information provided is either not specific enough to be useful or is a repeat of what has already been reported in the media. Larger companies, especially those with significant overseas operations, have very strong information-sharing relationships with the U.S. and foreign intelligence communities, but smaller companies, or those primarily domestic-based, have less robust means by which to receive threat information. There is also a clear distinction between types of intelligence required by industry, depending upon whether the private sector user has strategic or tactical responsibilities. National and global companies' strategic perspectives require broader threat information, whereas local facilities require tactical information about specific threats, methods, and timetables. Strategic intelligence sharing seems to be stronger than tactical intelligence sharing, but improvement is steadily being made on all fronts.

It was found that Federal Government intelligence about physical threats and vulnerabilities to the ONG Sector was far better than intelligence about cyber threats. Most of those interviewed stated that highly-valued cyber intelligence comes primarily from vendors, not the Federal Government, and that vendors are usually able to provide specific solutions to the problems identified.

4.1 Roles and Effectiveness of Primary Information Sources

Those interviewed reported that the sector uses multiple approaches to acquire intelligence information. There was no single source identified as the most important; rather, private sector analysts and security directors consult several intelligence sources and then integrate their findings. Sources of intelligence information cited in the interviews can be found in Figure ONG-2.

Figure ONG-2: Sources of Intelligence-Derived Information for ONG Sector

Source	Examples
Federal Government	• Classified briefings (regularly scheduled as well as special alerts), normally coordinated and/or conducted by DHS and held in Washington, DC or Houston, TX; often including the FBI • Meetings with TSA on pipeline and transportation issues • Information from the Federal Government to the ONG SCC; to member trade associations, and to member companies • The U.S. State Department's Overseas Security Advisory Council (mostly for international companies) • The FBI's Domestic Security Alliance Council
	• Personal contacts within the U.S. Intelligence Community (often because of past employment with an intelligence agency) • Communication with the ONG Sector Specialist, who is considered especially knowledgeable • DHS organizations such as IP, Office of Intelligence and Analysis (I&A), National Infrastructure Coordinating Center (NICC), and HITRAC • Visits to web-based information sources, such as HSIN-CS, HSIN-ONG, US-CERT, DOE ISERnet, FBI InfraGard, and the NIST Computer Security Resource Center

	• Collaboration with one or more of the Department of Energy National Laboratories • DHS Daily Infrastructure Reports • DOE data, such as the Energy Assurance Daily Reports
State and Local Governments	• State and local governments • Local law enforcement and mutual assistance groups, including regional response groups • Personal contacts with State Police and Joint Terrorism Task Forces • State and local fusion centers
Private Sector	• Joint briefings and meetings under the CIPAC umbrella between an ONG Working Group and the Chemical Sector • Monitoring current and breaking news through the media, especially CNN • Participation in and close interaction with the ONG SCC and its various Working Groups, such as the Intelligence Requirements Working Group • Contracted private-sector companies, such as Control Risks Group, ASI Group, Stratfor, and Olive Group, as well as various web-crawling firms • Personal contacts with larger ONG companies with international presence which maintain internal intelligence capabilities • Internal intelligence assets within the company, often staffed by former government intelligence analysts • Participation on security committees (both physical and cyber) within large industry associations, such as the American Gas Association, the National Petrochemical and Refiners Association, the Interstate Natural Gas Association, and the American Petroleum Institute • Frequent discussions with major vendors of cyber software and hardware (especially important for those responsible for IT in ONG companies) • The trade press
International	• Relationships with U.S. and foreign government intelligence agencies (mostly for international companies) • Informal conversations with Army personnel and others stationed in areas of interest to individual companies

Role of the Sector-Specific Agency

The ONG SSA works closely with the ONG SCC to ensure that the sector's concerns are relayed to the proper agencies within the Federal Government, and works with the Energy Sector Government Coordinating Council (GCC) to communicate the Federal Government's concerns to the sector. DOE is recognized as being an advocate for energy in government, so its role as SSA is natural and supported. DOE works with the ONG SCC to develop annual strategic plans, which are useful in articulating sector concerns to the Energy Sector GCC. Information sharing has been on the ONG Sector priority list for some time.

Threat information is the most important type of intelligence needed by the ONG Sector. The ONG SSA has been working within the sector and with DHS to improve the sharing of threat information, but challenges remain. These include:

- Security clearance management: The main problem is not the number of clearances but who in a given company holds the clearance. This is particularly true with respect to cyber security, where the clearance level must be very high to receive the intelligence provided by the Federal Government.
- Personnel turnover: People don't stay long in one position and, when they leave, their clearance goes with them, leaving a gap in cleared personnel within a department or company.

- Classified briefing implementation: While the content of and participation at classified briefings have been improving, not enough people on the private side have clearances or have the time to travel. When the briefings are held at the FOUO level, the information is often too general or already publicized through the media.
- Federal coordination: DOE needs to be involved right away on ONG-related incidents, but sometimes there are multiple agencies responding and they can get in each other's way. The ONG SSA does not have sufficient resources to place people directly in HITRAC.

The SSA has been helpful in participating in the DHS Sector Intelligence Needs (SINS) process, which is viewed as being promising because it involves collaboration between the sector and DHS intelligence analysts in identifying sector intelligence requirements. The ONG SSA also works with industry associations, but while large associations have very knowledgeable security experts, they operate under constraints and their interests are not always parallel to those of either the Federal Government or individual companies within the sector. Over time, the ONG SSA has built very strong, trusted relationships within the ONG Sector. One key is being sensitive to the private sector's proprietary information concerns. Ground rules have been established so information is not inadvertently leaked.

Role of the DHS ONG Sector Specialist

The DHS ONG Sector Specialist is an advocate for the sector within the Federal Government to address sector concerns and requirements. The primary responsibility of the Sector Specialist is to be NPPD/IP's liaison to the sector to coordinate a diverse set of activities, including information sharing. To do this effectively requires work and experience, plus an ability to understand the perspective of others.

The primary information-sharing tool for IP is HSIN – CS, which some ONG Sector participants use because it is cost effective. The ONG Sector Specialist has encouraged more people to use HSIN, but this effort has not been entirely successful because DOE, as the SSA, uses ISERnet. The sector wants actionable information that is timely and not otherwise available from open sources. The fact that the U.S. Intelligence Community is not focused on private sector critical infrastructure sometimes makes the sharing of intelligence information challenging. The approval process for the dissemination of intelligence takes too long, thereby negating much of its use to the private sector.

The ONG Sector Specialist coordinates sector requests for security clearances related to critical infrastructure protection, and passes them on for processing to another DHS organization. The review and approval process is improving, but a backlog still exists.

Role of State and Local Governments

We learned that, although each State handles critical infrastructure protection issues somewhat differently, some States separate protective measures from threat-based information, with the State fusion center bridging the separation in many instances. The building of personal relationships was important in the State context, because many State agencies were reluctant to share information except with those in industry whom they knew. Companies themselves were sometimes reluctant to share information with State agencies, unless a personal relationship had already been established. Some States (e.g., Washington, Maine, New Jersey) were said to have good intelligence-sharing relationships with energy companies.

State emergency managers reach out to different Federal Government sources for information. DOE situation reports were said to be extremely useful for specific incidents, such as hurricanes, but not very strong on assessments with broader implications, such as the situation in the Middle East. One problem with sharing information with the Federal Government was inconsistency in information sharing procedures, with guidance being changed constantly. Also, certain reports from DHS (e.g., Sector Annual Reports) were distributed at least one year late, thereby reducing their value to either State agencies or ONG facilities within their jurisdiction. It was noted that many larger ONG companies work closely with the Federal Government, but, even so, information received must be analyzed for its effects at the local level.

4.2 Information Sharing Mechanisms and Processes

Interviewees reported various levels of expectation and satisfaction with their preferred sources of information. Examples of discussions related to specific mechanisms follow.

West Virginia Fusion Center

ONG Sector interviewees reported several cases of success in bi-directional information sharing. One participant depicted an incident where a company employee working in a remote part of a rural State spotted an intruder on one of their properties. The intruder and his car and license plate were caught on camera. This employee contacted and shared this information with the West Virginia Intelligence Fusion Center. The fusion center identified the intruder and found that the intruder had been spotted in other energy properties throughout the State. The fusion center published this information in a weekly bulletin so other energy companies could increase their surveillance. The FBI then took over the investigation.

HSIN–CS and ISERnet

HSIN–CS is used by many companies, but not by all. It is not, in most cases, the primary source of information used. The quality of the information on this “pull” system has improved over the years.[56] Most users cited the strengths of HSIN as having good resources in its library and excellent training tools. It also was said to contain useful information about past incidents. As such, HSIN has become a site that larger firms with intelligence analysts use to collect information. In the Energy Sector, many companies use the secure DOE network, ISERnet, maintained by the DOE ISER division, for the same purposes.

Fusion Centers

Most of those interviewed did not have extensive contact with their local fusion centers. Those that did were most satisfied with their participation if: 1) the center had a strong collaboration mission with the private sector, 2) the center was relatively mature and well staffed, 3) strong personal or organizational relationships had been built between the industry and the center, 4) there existed a leadership catalyst to make public-private collaboration work within the fusion center, and 5) useful products were being disseminated.

Some interviewed thought that the fusion centers served only their own intelligence needs (primarily law enforcement), voicing the opinion that they were unclear as to what useful information the fusion centers could provide them. What they did not want was more redundancy in information. Often, even though the reputation of a local fusion center was good, the company had existing information sharing contacts elsewhere (e.g., directly with local law enforcement) and tended to continue to use those rather than reach out to the center.

Those interviewed frequently said that the fusion centers should have more subject matter experts so the centers could better understand the impact of intelligence information on industries in their jurisdiction. The observation that each fusion center had its own idiosyncrasies and lacked a common model also was expressed by several of those interviewed. It was recommended that fusion centers

[56] “Pull” information systems refer to those from which the user has to request certain data. “Push” systems, by contrast, refer to those that deliver data directly to the user without the user specifically requesting the data.

reach out to State agency subject matter experts to learn about a sector before initiating contact or trying to establish information exchanges with the industries concerned.

Fusion centers identified by name as being models for public-private information sharing and cooperation included:

- West Virginia Fusion Center
- Indiana Intelligence Fusion Center
- Arizona Counter-Terrorism Intelligence Center
- Houston Regional Intelligence Service Center
- New York City Fusion Center

Classified and Unclassified Briefings

There are classified briefings on a variety of subjects of interest to the ONG Sector, including formal ONG SCC classified briefings, Chemical Sector/ONG Sector joint classified briefings, and Pipeline classified briefings. Many of those interviewed participated in or knew about two major classified briefings held by DHS, usually in Washington, DC. The quality of the briefings has greatly improved over the years and the sector generally finds them to be very useful. The value of the briefings has increased because the ONG Sector Specialist makes a point of reaching out to ONG representatives to find out what they need to hear. Some expressed the view that more chief executive officers and chief security officers should attend the briefings, because senior management does not fully understand the severity of some of the threats facing the industry.

Some interviewed suggested that a better cyber threat and vulnerability lexicon should be built into the briefings. Some voiced the opinion that DHS is extremely poor in terms of the quality of cyber security intelligence and information shared with the sector, and doubted it could be improved unless a champion emerged at DHS to improve its cyber security programs.

Threat briefings held over secure lines with DHS or in more convenient locations closer to their company headquarters also were favorably received. Monthly FOUO DHS teleconferences on suspicious activities and trends are improving as they have become more interactive. For example, some of those interviewed noted with satisfaction the periodic unclassified teleconference calls with the TSA Pipeline Working Group and joint calls with the Chemical Sector.

Local Law Enforcement and Joint Terrorism Task Forces

Most of those interviewed reported good working relationships with State and local law enforcement and also with their local FBI-sponsored Joint Terrorism Task Force (JTTF). Some companies reported frequent contact with local law enforcement and regional JTTFs on crime-related issues, terrorism, and requirements for first responders. At the National level, FBI collaboration with private sector security officials in the Domestic Security Alliance Council was mentioned as being very useful. Companies with port facilities also have close working relationships with the local U.S. Coast Guard and with local Customs and Border Patrol offices.

In-House Analysts

There has been a recent trend among major ONG corporations to hire full-time intelligence analysts to work within the company. We found these corporations to be very sophisticated in their analysis, with many former government employees (including those from intelligence agencies) assessing information flows from many sources. In some cases, for example, companies have identified those threat profiles which they believe to be of greatest concern. Most companies within the sector, however, did not have these capabilities and relied instead on information available from the Internet, trade associations, vendors, personal contacts, and other non-classified sources for the bulk of their needs.

Personal Contacts

Despite multiple, formal mechanisms for acquiring intelligence-derived information, the most frequently used method to share critical information appears to be personal contacts developed over the years. Many of those interviewed noted that the individuals in their industry dealing with specific types of threats (such as cyber security or terrorism) were few in number and therefore were known by everyone in the same field. This contributed to a sense of trust and mutual benefit that greatly facilitated security-related information exchange in the sector.

These personal contacts create an informal network connecting individuals who themselves have access to various intelligence and information sources. Key information sometimes comes through industry associations, the ONG SCC, personal contacts within the Federal Government, law enforcement, other companies, and other sources. Industry security personnel tend to reach out to people they know to develop additional information on known issues or to receive alerts that they might have otherwise missed. It is an informal system of information exchange, but it works fairly rapidly and enables individuals in the industry to assemble multiple pieces of information into useful intelligence.

Factors Influencing the Private Sector's Willingness to Share Sensitive Information with Government

The ONG Sector shares two types of information with government: regulatory and voluntary. For example, ONG Sector companies are required by law to share information and intelligence with the U.S. Coast Guard under MTSA. This kind of information includes the reporting of incidents and Suspicious Activity Reports (SARs) to the National Response Center. The voluntary sharing of information with the Federal Government, such as with DHS (NICC or Transportation Security Operating Center), raises liability, privacy, and competitive concerns within industry.

Those interviewed felt that the exchange of sensitive information between the private sector and the Federal Government had improved greatly, in large measure because the ONG Sector understands that they are part of the intelligence process. The agency within the Federal Government with which intelligence-related information was shared varied. One key variable seemed to be the degree of trust in a given agency—often built over a considerable period of time and frequently with a single point of contact within the agency. The fact that so many agencies and offices within the government receive and provide information is a problem to some companies, because they are not sure with whom to deal on any given subject, nor are they sure how the information will be shared within government itself.

Abqaiq Attack

In 2006, a major Saudi oil facility was attacked by al Qaeda terrorists. Two suicide bombers attempted to drive two cars packed with explosives into the oil facility. The attack was thwarted by heavy security. ONG security specialists reviewing the incident noted their interest in what motivated the attack, the mode of attack, and what caused the attack to fail. This intelligence would assist American ONG companies to properly allocate resources to prepare and protect similar facilities in the United States. Although the event occurred outside of the United States, this kind of analysis would be greatly beneficial to the ONG Sector.

In all cases, companies reported a much more productive information-sharing relationship when their government counterpart (usually an individual) was knowledgeable of their sector. As a whole, the ONG Sector did not feel that the Federal Government fully understands the sector's intelligence requirements. This was reflected especially in the area of cyber security, where industry representatives reported that the quality of information received from the government was far less useful than that received from vendors—except in very specific cases dealing mostly with vulnerabilities in control systems and other more highly sophisticated cyber security threats.

Some larger companies provide information to the NICC on a 24/7 basis and receive threat information directly in return. The companies review the information received from the NICC, and then may route that information through various channels, such as regulatory agencies (generally only when required), other local facilities, and the JTTF when appropriate. These types of companies feel very comfortable with information sharing mechanisms with government and with their reporting requirements to regulatory agencies.

The willingness to share information voluntarily with government was driven in large measure by its utility to the company: if the information received from the government was useless or the company perceived that information it provided was not valued or acted upon, then it was not inclined to participate further. Also, companies were very sensitive over State sunshine laws and not knowing what information in each State will be subject to public disclosure. If sensitive information were leaked or perceived to be used inappropriately, then again the company concerned would not be inclined to participate further. The ONG Sector is sensitive to the exchange of intelligence information with government because the sector is heavily regulated, full of anti-trust issues, highly liable, and concerned over the lack of information protection. Nonetheless, when important intelligence-related information does come to their attention, sector members are usually very willing to share it with government.

Counterintelligence

Those interviewed reported very little counterintelligence sharing with government, except in cases where 1) companies were involved with overseas operations, or 2) companies were trying to protect their reputations or trade secrets. The sharing of counterintelligence across the sector itself is very limited. Those that engage in counterintelligence activities usually do so from the perspective of business counterintelligence in monitoring competitors. Accordingly, some of those interviewed stated that counterintelligence should be an internal company responsibility: they should educate their own personnel on how to protect proprietary information.

5.0 Findings

In reviewing the data collected in this case study through interviews and open source research, we believe the following 10 findings best summarize the status of intelligence sharing from the perspective of the ONG Sector:

Finding 1: Oil and Natural Gas

Despite overall improvement, there remains a gap between the intelligence information that the Intelligence Community (IC) provides the ONG Sector and the type of intelligence that the industry needs for its planning and operations.

To some extent, there also exists a gap between what the sector believes the IC can provide and the type of intelligence that the IC actually possesses. Both the sector and the IC are working to clarify needs and expectations, For example, owners and operators do not always need finished intelligence products, but rather want timely information that they can use to improve facility security. Industry values even unvalidated IC information because sector analysts can pull from preliminary findings and fragmentary information the details specific to their own operations. Too often, the IC validation process delays intelligence sharing with the private sector, who ultimately receives information that is then outdated and not of great value.

The U.S. Intelligence Community (IC) needs to move out of the "Cold War mentality" into an era of intelligence and information sharing with critical infrastructure that is much more robust.[57] Identifying sector-specific intelligence requirements (such as the Sector Intelligence Needs [SINS] process being developed by the ONG Sector and DHS) should be elevated as a priority within DHS as well as other members of the IC.

Finding 2: Oil and Natural Gas

There is a considerable difference between the quality and quantity of intelligence received by smaller and larger ONG companies.

Smaller companies have fewer resources to devote to security and intelligence, so they tend to leverage what is readily available through government resources such as local law enforcement, the FBI, local fusion centers, and HSIN-CS. Larger companies have a higher risk exposure and can allocate more resources to intelligence collection and analysis. Their sources include a much wider range of government contacts, as well as private security/intelligence firms and corporate-owned intelligence collection and analysis.

Finding 3: Oil and Natural Gas

ONG Sector representatives require more security clearances across the sector, especially for those individuals addressing emerging threats such as cyber security.

The private sector grows increasingly concerned that many industry cyber security personnel do not hold clearances and therefore cannot attend classified briefings in which vital cyber security issues are discussed. The speed with which threats are detected and need to be countered, the expanding use of cyber systems to manage key aspects of the industry (e.g., SCADA and other control systems), and the lack of security clearances among industry cyber operators are factors contributing to a growing sense of cyber vulnerability in the sector. Because vendors are frequently the first partner industry calls when it has a cyber problem, vendors need to be included as part of the intelligence and information sharing process. US-CERT provides general, less-targeted information used to guide strategy to help shape security programs, whereas vendors can provide specific information for "zero-day" situations requiring an immediate response.

Finding 4: Oil and Natural Gas

Because security clearances limit who can receive information and how widely they can share it, ONG Sector owners and operators request that DHS and other IC components complement classified information sharing with more frequent unclassified briefings and For Official Use Only (FOUO) materials that can reach more decision-making and operational personnel.

The sector also requests that presenters at classified briefings prepare unclassified summaries of their material for wider distribution within the sector.

Finding 5: Oil and Natural Gas

The sharing of counterintelligence across the ONG Sector is very limited due to confusion over the term and concerns over the regulatory and business repercussions of sharing.

[57] The so-called "Cold War mentality" refers to a mindset developed during the Cold War wherein components of the Intelligence Community were highly compartmentalized in order to avoid penetration by spies and damaging leaks that could comprise intelligence sources and methods.

Private sector owners and operators are uncertain as to what counterintelligence actually means. Both large and small companies tend to avoid sharing counterintelligence with all levels of government within the context of domestic operations because of concerns over negative publicity, liability issues, and a desire to protect proprietary information. There also may be regulations that prohibit information sharing, such as antitrust laws, and particularly information pertaining to pricing and/or supply interruption. Companies fear putting their competitive advantage at risk. However, multinational companies within the ONG Sector often cooperate with the U.S. Government in counterintelligence within the context of their overseas operations.

Finding 6: Oil and Natural Gas

The ONG Sector uses a wide range of information sharing tools and mechanisms to get the information they need.

Owners and operators value the Homeland Security Information Network – Critical Sectors (HSIN-CS) primarily as a reference tool, finding it unable to provide the timely, relevant data to support operational, real-time security. Other information mechanisms include local fusion centers, the DHS Protective Security Advisors and the ONG Sector Specialist, the Transportation Security Operations Center, local Joint Terrorism Task Forces, FBI, local law enforcement, US-CERT, the ONG SCC, trade associations, contracted private intelligence companies, and others.

Finding 7: Oil and Natural Gas

ONG companies with global interests have inherently more complex security and information needs, requiring active intelligence sharing with U.S. Government agencies.

Key partners include the State Department, CIA, DoD, DHS, and others. The sector particularly values the State Department's Overseas Security Advisory Council (OSAC). Most global companies also maintain close working relationships with foreign governments, including law enforcement and other security agencies.

Finding 8: Oil and Natural Gas

The use of fusion centers as an information-sharing mechanism varies considerably across the ONG Sector, and most interaction occurs at the local facility level rather than with a company's corporate headquarters.

Often, involvement with the fusion centers relies on personal relationships to build effective bi-directional information-sharing partnerships. There is wide recognition of the potential value of working more closely with fusion centers, but the lack of consistency in these centers, in terms of both services and personnel, tends to hamper cooperation. Recent initiatives such as the DHS Joint Critical Infrastructure Partnership (JCIP) Regional Symposium events hold promise in improving fusion center/industry communications. One outstanding private sector and fusion center partnership is the West Virginia Intelligence Fusion Center, which the sector considers to be a model for other centers looking to improve outreach efforts to the private sector.

Finding 9: Oil and Natural Gas

The lack of government feedback on the information shared by ONG companies frustrates the private sector and decreases incentives to share.

The ONG Sector recognizes a value in voluntarily sharing intelligence information with the government, but a company rarely knows whether the intelligence it shares is useful or has an impact on their operations. This lack of a feedback loop reduces the private sector's interest or perceived value in sharing intelligence over the long term.

Finding 10: Oil and Natural Gas

Collaboration between the ONG Sector and DHS (both I&A and IP) to define the sector's intelligence information needs is welcomed by both parties and shows promise in improving intelligence information sharing between the sector and government.

6.o Conclusions

The members of the ONG Case Study believe the following seven conclusions are of the highest priority to the ONG Sector at this time:

Conclusion 1: Oil and Natural Gas

DOE and DHS should work closely with sector owners and operators to finalize an agreed-upon set of intelligence information requirements for the sector and ensure intelligence analysts have sufficient sector expertise.

Intelligence requirements should include a description of the type of information needed by the sector, such as potential attacker motivation, likely targets, and probable mode of attack. As part of this process, DOE and DHS should institute training and/or educational programs to inform members of the Intelligence Community (IC) and the sector of each other's information sharing requirements and expectations. Government should provide sector-specific training to both government and industry intelligence analysts, with the following elements:

- The training will ensure that government analysts know what to look for (e.g., what sector interdependencies exist, what geographic areas are of particular interest) to enable them to provide useful intelligence to the sector. The training also would inform ONG Sector analysts and security directors of what information they can realistically expect from government.
- Government should work toward consistency and long-term expertise for sector-specific analysts within the IC. The IC needs to shift from using generalists to sector specialists so that discussions with the private sector can focus on details rather than basic sector operations. One suggestion was to embed IC analysts in the ONG Sector for rotational assignments, as the IC often integrates private sector expertise. These analysts, once returning to their parent organization, would better understand sector-specific risks and what types of risk are acceptable or unacceptable to industry.

Intelligence requirements and training should aim to narrow the gap between sector expectations and Federal Government capabilities to provide actionable intelligence to the sector. To further serve this purpose, industry can expand upon its program of inviting government intelligence personnel on tours of ONG facilities, and the government can provide training to owners and operators on information-sharing protocols, including why certain levels of information can't be shared.

Once requirements are better understood, DHS, DOE, and other agencies, should clearly direct the sector to where specific threat and risk information can be obtained on a timely basis. The sector communicates on a regular basis with multiple Federal agencies that both provide intelligence and request information about the sector's operations. Federal agencies roles, especially as they relate to intelligence, are often unclear to industry and should be more clearly defined so that the private sector knows where to go with threat concerns.

Requirements development is under way through the Sector Intelligence Needs (SINs) process being developed by the ONG Sector and DHS. Pending a successful outcome, the process may serve as a model for other sectors that need to more clearly define their intelligence needs and improve intelligence information sharing with the Federal Government. Effectiveness of the process hinges on whether or not the product is widely disseminated and acted upon. This information could be shared with fusion centers as they develop their local SINS and thereby eliminate duplication of efforts.

Conclusion 2: Oil and Natural Gas

DOE and DHS should work closely with the sector and the IC to develop a formal program of ongoing intelligence briefings and publications at the For Official Use Only (FOUO) level to enable the wider dissemination of actionable information that enables the private sector to proactively implement security enhancements in their specific facilities and areas of expertise.

Government should work to provide more FOUO documents for non-cleared industry personnel. The sector strongly recommends that all classified briefings have, as a deliverable at the end of the presentation, an unclassified summary that industry participants can distribute to others within their companies.

Conclusion 3: Oil and Natural Gas

DOE and DHS should continue to expedite the security clearance process for need-to-know owners and operators, managers, and employees of the ONG Sector.

- DOE, DHS, and other classified information providers should expedite the delivery of classified information to the sector by improving ONG Sector access to both security clearances and better processes and mechanisms for classified information dissemination:
- Government should increase the number of security clearances for industry personnel, especially for those working in cyber security. Cyber security threats increase while a large portion of ONG cyber security personnel are not privy to time-sensitive information in classified briefings. One option to mitigate this is to create a special category of clearances for cyber security experts. The government also should improve its communications with industry on the status of clearances currently in process. The current security clearance backlog should be reduced, starting with the applications of ONG security directors.
- Local Sensitive Compartmented Information Facilities (SCIF), secure phone lines, and fusion centers have been used in the past and their use could be enhanced to promote expeditious sharing of information.

Conclusion 4: Oil and Natural Gas

The Intelligence Community, led by DHS, should work to provide more targeted classified and unclassified threat information that provides value based on sector-specific risks and needs.

The Federal Government can improve its classified briefings and unclassified information products by adopting an interactive environment with the ONG Sector to determine, prior to the meetings, what intelligence the sector actually needs to receive. Government should provide complementary information about possible mitigation strategies to address the threats and vulnerabilities brought to the attention of the sector. The following specific recommendations can together improve the content of classified briefings to offer ONG security directors and executives more value:

- Government should provide a checklist of possible vulnerabilities in its classified cyber reports so companies can more easily identify what components of their systems might be vulnerable.
- Government should provide more intelligence and actionable information about supply-chain issues, including those involving global activities.

- Government should encourage wider participation by ONG Sector senior executives in classified briefings to increase their understanding and appreciation of the magnitude of threats their industry is facing—especially emerging cyber threats that are well-funded and insidious. Such exposure would help inform key decision-making within the industry.
- Government should brief private industry on closed investigative cases, enabling them to develop threat profiles, including the motivations of the actor, how the target was chosen, the mode of attack, and what led to success or failure of the attack.
- Government should report compromised web sites to the private sector, so industry can take defensive measures to shut them down rather than have their information compromised.
- DHS and other members of the IC should compile and present in briefings strong case studies on global events that could apply to the ONG Sector domestically. Often, the sector finds out about these incidents from foreign governments or other overseas contacts. The Chemical Sector classified briefings were identified as a model.
- Government should enhance intelligence and information filtering so facilities don't receive messages that don't apply to their assets or operations. Unless interdependencies are involved, ONG facilities should not receive information about other sectors' vulnerabilities.

Conclusion 5: Oil and Natural Gas

DOE and DHS should develop a "one-stop shop" where sector owners and operators can obtain FOUO intelligence products relevant to the industry. Fusion centers and other locations that develop local products could be integrated into such a repository. There are many companies within the sector that have assets widely distributed across many States that are managed by a National/centralized security staff. Currently, there are multiple locations the private sector must use to try to find information (e.g., InfraGard, HSIN, fusion centers). A recommended model for public-private sector collaboration is the State Department's Overseas Security Advisory Council (OSAC), a model which the FBI is following in the establishment of its Domestic Security Alliance Council.

Conclusion 6: Oil and Natural Gas

DHS should take the lead in integrating the fusion centers with the private sector to improve coordination with local and National intelligence products. Most fusion centers do not have private sector representation. DHS could utilize the ONG SCC to facilitate vertical penetration and outreach between the sector and fusion centers. Individual ONG facilities should proactively seek to establish cooperative relationships with their local fusion centers.

Conclusion 7: Oil and Natural Gas

DOE, DHS, and the Department of Justice should work with the sector to streamline and integrate information sharing mechanisms to ensure that: 1) industry has a single point of contact to which to send information and 2) a robust feedback loop provides industry information on how the information they provide was used.

Currently, there are duplicative or unclear expectations as to which agency the sector should send its incident reports, and companies tire of answering the same questions for multiple Federal agencies in an event. Agencies should work together to develop a streamlined information sharing mechanism and reporting requirements that enable companies to share pertinent information using one avenue that reaches multiple agencies, including relevant law enforcement and intelligence groups. Currently, the NICC, TSOC, NRC, and JTTFs currently are likely to all be notified separately. It should also address concerns regarding antitrust issues, potential liabilities for reporting, anonymity in reporting, and processes for sharing the information readily within the sector.

Government should also work toward consistency in its regulations, rather than expecting companies to work with a multiplicity of agencies acting under different regulations (e.g., some ONG facilities operate under MTSA as well as the Chemical Facility Anti-Terrorism Standards and the Coast Guard's Transportation Worker Identification Credential). One of those interviewed, for instance, pointed to duplication between programs of the TSA Pipeline SCC and the ONG SCC. The confusion and duplication of efforts that results from trying to adhere to regulations from multiple agencies tends to reduce the flow of information from the private sector rather than increase it. Government response should also be consistent. The National Threat Advisory System should match the maritime security threat levels in order to simplify the process for global companies operating in numerous sectors and geographic areas.

Finally, DHS should develop a process to ensure that feedback is provided to the private sector on the suspicious activity reported. DHS should establish protocols for following up with the ONG reporting entity, and provide specific timelines on when to expect response. This would help ensure that both the IC and the ONG Sector understand whether the information they provide is valuable and increase the usefulness of the reports each generates.

Appendix G. Other Pertinent Studies on Information Sharing

The NIAC found a number of reports whose findings and recommendations are quite similar to those in this NIAC report. Two in particular are:

- Intelligence and National Security Alliance and Homeland Security Intelligence Council (INSA), "Intelligence to Protect the Homeland…Taking Stock Ten Years Later and Looking Ahead," September 2011, https://images.magnetmail.net/images/clients/INSA/attach/INSA_Homeland_Security_Intelligence.pdf
- Markle Foundation, "Meeting the Threat of Terrorism: Culture Change: New Thinking on Information Sharing Critical to Strengthening National Security," September 1, 2009, http://www.markle.org/sites/default/files/MTFBrief_CultureChange.pdf.

Other related studies include:

- U.S. Government Accountability Office, Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investments, GAO-11-455, July 2011, http://www.gao.gov/new.items/d11455.pdf.
- U.S. Government Accountability Office, Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results, GAO-10-972, September 2010, http://www.gao.gov/new.items/d10972.pdf.
- U.S. Government Accountability Office, Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure, GAO-11-865T, July 26, 2011, http://www.gao.gov/new.items/d11865t.pdf.
- National Security Preparedness Group, "Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations," September 2011, http://www.bipartisanpolicy.org/sites/default/files/CommissionRecommendations.pdf.
- DHS, Office of Inspector General, Information Sharing with Fusion Centers Has Improved, but Information System Challenges Remain, OIG-11-04, October 2010, http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_11-04_Oct10.pdf.
- Markle Foundation, "Nation At Risk: Policy Makers Need Better Information to Protect the Country," March 1, 2009, http://www.markle.org/sites/default/files/20090304_mtf_report.pdf.
- Markle Foundation, "Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trust Information Sharing Environment," July 1, 2006, http://www.markle.org/sites/default/files/2006_nstf_report3.pdf.

A few selected quotes from the INSA study and the Markle Foundation white paper on meeting the threat of terrorism are cited below:

Intelligence and National Security Alliance and Homeland Security Intelligence Council, "Intelligence to Protect the Homeland…Taking Stock Ten Years Later and Looking Ahead," September 2011.

> In the aftermath of the tragic events of 9/11, Americans slowly came to the realization that while the country had spent considerable national treasure on intelligence capabilities over the years to protect the nation and had prevailed in the Cold War for which the U.S. Intelligence Community (IC) had largely been designed, this IC was not designed, equipped, or ever primarily

> intended to detect significant national security threats originating or residing within our nation's own borders. (p. 3)
>
> When it comes to protecting the nation from a terrorist attack, the relevant intelligence collectors, analysts, and the final decision makers will be in different agencies and departments at different levels of government or within the private sector in some cases (e.g., when the threat vector is a cyber attack on the nation's critical infrastructure). At the same time, intelligence generated for one operational entity may have relevance to more than one [Homeland Security Intelligence] Enterprise member—in many cases in a way that was not originally understood by the original analyst. Unity of effort among the disparate members of the Enterprise accordingly requires development of a networked approach, such as the one established among the 72 State and major urban area fusion centers working with FBI Field Intelligence Groups (FIGs) and Joint Terrorism Task Forces (JTTFs) and connected to DHS I&A and NCTC [National Counterterrorism Center]. Such a networked structure will facilitate a linkage that promotes an effective, disciplined, common system for requesting information and receiving a response. To optimize this unity of effort, all elements of the Enterprise including nontraditional partners of the IC, such as other Federal agencies, (e.g., Transportation Security Administration, Immigration and Customs Enforcement, and Customs and Border Protection), as well as State, local, and tribal law enforcement partners, should share common analytical training standards. (p. 9)
>
> I&A serves as the executive agent for leading Federal Government-wide support for fusion centers and has helped coordinate the provision of Federal funding, technical assistance, security clearances, and access to classified networks. Additionally, DHS has assigned intelligence liaison officers to most fusion centers with the mission to support their analytical efforts, facilitate information sharing between the Federal Government and State, local, and tribal partners, and provide training. There has been important progress since fusion centers were established by State and local governments in the years following September 11, 2001, but capability building to a common standard among all centers remains a challenge due to diminishing budgets at the State and local level and a shortage of trained intelligence analysts. (pp. 9-10)
>
> HSI [Homeland Security Intelligence] will have fully developed as a distinct intelligence discipline when it functions seamlessly as an analyst-to-analyst system across organizational boundaries. At that point, it will reach its highest value in protecting the homeland from significant threats, particularly terrorism. The system will require unique, and not yet identified, analytic frameworks, knowledge management, collaboration tools, and training that include built-in safeguards for privacy, civil rights, and civil liberties protections for U.S. persons. Over time, the system would optimally build new information sharing platforms and technical solutions. Until that time, it will rely on smart analysts communicating and sharing to the best of their ability in a manner that meets applicable legal, regulatory, and policy guidance. (p. 11)

Recommendations of the INSA report include: (pp. 16-17)

- The President, Congress and the Director of National Intelligence (DNI) should embrace a Homeland Security Intelligence Enterprise (Enterprise) characterized by fully connected federal, State, local and tribal law enforcement and public safety agencies, as well as private partners as required, with broadly defined and overlapping counterterrorism responsibilities focused on the coordination of intelligence and analysis efforts, not hierarchical command and control.

- To ensure unity of effort within the Enterprise, the President and Congress should reaffirm the critical role of the DNI in providing strategic direction, coordinating homeland security intelligence activities, setting standards, and establishing priorities to drive collection and the development of required capabilities.
- The DNI, in coordination with the Secretary of Homeland Security and the Director of the FBI, and in consultation with State, local and tribal leaders, should develop and implement foundational analytical training standards across the Homeland Security Intelligence Enterprise to ensure mission partners have common skills and understanding to communicate and collaborate.
- The DNI, in partnership with the DHS Office of Intelligence and Analysis, the Director of the FBI and State, local and tribal leaders should articulate a clear, lawful role for fusion centers in the national intelligence process and the national intelligence strategy, and define what constitutes appropriate Federal presence in a fusion center. DHS I&A as the Federal executive agent, should establish standards for training all fusion center analysts to a common analytic standard.
- The Program Manager-Information Sharing Environment should promote a decentralized environment in which disparate analytic nodes can communicate with each other and share knowledge. Technology should be the enabler but should not replace the analyst. New technology is not necessarily required but rather more effective integration and optimization can be made of existing systems and those under development.
- The DNI should develop and recommend policies that foster greater connectedness and eliminate barriers to legal information sharing and collaboration among the tens of thousands of Federal, State, local, tribal, and private sector entities that comprise the Enterprise.

Markle Foundation, "Meeting the Threat of Terrorism: Culture Change: New Thinking on Information Sharing Critical to Strengthening National Security," September 2009.

> Developing the effective information sharing framework critical to national security demands fundamental change in the culture of information sharing…..A change in culture and thinking will encourage a collaborative environment with a clear purpose: ensuring that those who need it have access to the best information in a timely manner and under the appropriate conditions to enable the most informed decision. A network environment that truly facilitates information sharing is a combination of people, processes, policies and cultures that leverages advances in information technology and the best thinking about how to mobilize information to improve decision-making and policy implementation across the government (pp. 1-2)

Recommendations from this white paper include: (pp. 1-2)

- Focus on people and policies, not just technology, because the fundamental hurdles to information sharing are not technical—they are cultural and well established in how people think and work.
- Change thinking from "need to know" to "need to share" to drive a virtual reengineering of how government works, increasing collaboration and allowing communities of interest to form across parts of the government while protecting privacy and civil liberties and preventing misuse and abuse.
- Recognize the risk of not sharing information while being sensitive to the risks of inappropriate disclosure.
- Address the needs of information consumers while addressing the security concerns of information collectors. Those who depend on information to make decisions and accomplish

their mission must be empowered to drive information sharing to ensure they get the best possible data.

- Incentives to improve performance would link program funding or individual promotion with an agency's performance mobilizing information. For example:
    - Integrating information sharing into performance reviews and budget and personnel resource allocation for all agencies with a national security mission so that agencies failing to act to mobilize information would get less funding.
    - Creating an information sharing award for the agency or unit within an agency most successful at making data discoverable, highlighting the value of information sharing to national security.
    - Increasing joint duty in the intelligence community to build a sense of trust and community, with promotion to senior levels requiring a tour of duty at another agency.

Appendix H. DHS Authorities in Intelligence Information Sharing

Introduction

This appendix addresses the legal authority of the Department of Homeland Security (DHS) to establish inter-agency procedures for sharing intelligence and homeland security information with the private sector. The information provided in Figure 1 summarizes the laws, policies, and strategies and implementing structures behind DHS's authority over public-private intelligence and information sharing. The Analysis section provides an in-depth breakdown of laws that give DHS explicit authority to establish information-dissemination procedures and laws giving overlapping authority to the Office of the Director of National Intelligence (ODNI) and the Department of Justice (DOJ) to establish similar procedures. The only firm conclusions that can be drawn are that the Secretary of Homeland Security (DHS Secretary) has the authority to establish inter-agency procedures for disseminating unclassified and classified homeland security information to the private sector and that the Director of National Intelligence (DNI) has no authority over the direct dissemination of information to private-sector entities.

Please note that "intelligence," "homeland security information," and "terrorism information" are referenced in the text of this appendix in accordance with the term that was used in the corresponding law or policy. Given that great similarities exist between these three types of information,[58] this appendix discusses laws and policies that reference one or all of the terms.

[58] "National intelligence," "homeland security information," and "terrorism information" are defined as follows:

> The terms "national intelligence" and "intelligence related to national security" refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that—
>
> **(A)** pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and
>
> **(B)** that involves—
>
> **(i)** threats to the United States, its people, property, or interests;
>
> **(ii)** the development, proliferation, or use of weapons of mass destruction; or
>
> **(iii)** any other matter bearing on United States national or homeland security.
>
> 50 U.S.C. § 401a(5) (2006).
>
> The term "homeland security information" means any information possessed by a Federal, State, or local agency that—
>
> **(A)** relates to the threat of terrorist activity;
>
> **(B)** relates to the ability to prevent, interdict, or disrupt terrorist activity;
>
> **(C)** would improve the identification or investigation of a suspected terrorist or terrorist organization; or
>
> **(D)** would improve the response to a terrorist act.
>
> 6 U.S.C. § 482(f)(1) (2006).
>
> The term "terrorism information"—
>
> **(A)** means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities, relating to—
>
> **(i)** the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;

(Continued)

38 (Continued)

> **(ii)** threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;

Figure 1: Major Authorities for Public-Private Intelligence and Information Sharing

Law	**Homeland Security Act of 2002**	Created Department of Homeland Security. Required President to implement procedures for Federal agencies to share classified and unclassified homeland security information with appropriate State and local personnel (i.e., private-sector entities).
	Intelligence Reform and Terrorism Prevention Act of 2004	Established Office of the Director of National Intelligence (ODNI) to coordinate intelligence and information sharing within the Federal Government. Directed President to establish Information Sharing Environment (ISE) with policies and procedures for sharing terrorism information with the private sector.
	Implementing Recommendations of the 9/11 Commission Act of 2007	Required DHS Secretary to establish department-wide procedures to receive and analyze intelligence from State, local, and tribal authorities, and the private sector. Specified authorities for DHS Under Secretary for Intelligence and Analysis to integrate and standardize Department intelligence components. Required DHS Secretary to establish a fusion center initiative and provide intelligence advice and analysis to fusion centers. Created Interagency Threat Assessment and Coordination Group (ITACG) to set processes to share intelligence information with State and local governments and the private sector within ISE.
Policy	**HSPD-7 (2003)**	Defined critical infrastructure protection (CIP) responsibilities for DHS and SSAs. Directed DHS to establish uniform policies for integrating Federal CIP and risk management activities across all 17 (now 18) CIKR sectors.
	Executive Order 13311 (2003)	Delegated the functions of the President under Section 892 of the Homeland Security Act to the Secretary of Homeland Security.
	Executive Order 13388 (2005)	Directed agencies to give highest priority to developing information systems and disseminating intelligence-related information to fellow agencies, State and local governments, and private-sector entities
Strategy and Implementing Structure	**NIPP (2006, 2009)**	Established risk management framework across government and CIKR sectors. Defined sector partnership model and delineates roles and responsibilities.
	PM-ISE Information Sharing Environment Implementation Plan (2006)	ISE Plan established specific objectives for the sharing of terrorism-related information with the private sector.
	National Strategy for Information Sharing (2007)	Integrated ISE-related initiatives.

(iii) communications of or by such groups or individuals; or
(iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and
(B) includes weapons of mass destruction information.
6 U.S.C. § 485(a)(5).

Analysis

Section I addresses DHS's authority to create inter-agency procedures for the dissemination of homeland security information to the private sector. Section II discusses ODNI's origins and structure, as well as its authority to manage and direct the dissemination of intelligence information throughout the United States Intelligence Community (IC). Lastly, Section III reviews the Information Sharing Environment (ISE) and its authority structure with respect to the dissemination of information to the private sector.

I. DHS Authority

Section 892 of the Homeland Security Act of 2002 (Homeland Security Act) (6 U.S.C. § 482) covers the facilitation of information sharing procedures. **Subsection 892(b)** specifically deals with the sharing of homeland security information with State and local personnel. It states that "[u]nder procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate *State and local personnel* . . "[59] **Subsection 892(c)**, moreover, deals with the sharing of classified information and sensitive but unclassified information with State and local personnel. It states that "[t]he President shall prescribe procedures under which Federal agencies may, to the extent the President considers necessary, share with appropriate *State and local personnel* homeland security information that remains classified or otherwise protected . . ."[60] "State and local personnel" means "[e]mployees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government . . ."[61] Therefore, through the Homeland Security Act, the President was given the responsibility of establishing inter-agency procedures for sharing unclassified and classified homeland security information with appropriate private-sector entities. In addition, Section 892 supports DHS's ability to request IC elements to release intelligence information from their agencies so that such intelligence can be disseminated to the private sector through the procedures established by DHS.

Executive Order 13,311 (EO 13,311)[62] delegates almost all functions of the President under Section 892 of the Homeland Security Act to the DHS Secretary.[63] The functions not assigned to the DHS Secretary are the President's functions under Subsections 892(a) (2) and 892(b) (7), which entail ensuring that the procedures established for determining the extent of sharing homeland security information apply to all Federal Government agencies[64] and determining which Federal agencies shall review, assess, and integrate information shared by the State and local personnel.[65] After EO 13,311 became effective in July of 2003, it was amended by Executive Order 13,388[66] but never revoked. EO 13,311 is therefore still in effect and for other purposes delegates the President's authority to the DHS Secretary to prescribe

[59] 6 U.S.C. § 482(b)(1).

[60] *Id.* § 482(c)(1).

[61] *Id.* § 482(f)(3)(F).

[62] Exec. Order No. 13,311, 68 Fed. Reg. 45,149 (July 29, 2003).

[63] "In performing the functions assigned to the Secretary . . . the Secretary shall coordinate with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Energy, the Director of the Office of Management and Budget, the Director of Central Intelligence, the Archivist of the United States, and as the Secretary deems appropriate, other officers of the United States." *Id.* § 1(e).

[64] Homeland Security Act of 2002, Pub.L. 107-296, Title VIII, § 892, 116 Stat. 2253, 2253 (2002).

[65] *Id.* § 892, at 2254.

[66] Exec. Order No. 13,388, 70 Fed. Reg. 62,023 (Oct. 25, 2005). EO 13,311 was amended by replacing "Director of Central Intelligence" with "Director of National Intelligence" and replacing "103(c)(7)" with "102A(i)(1)."

procedures for Federal agency dissemination of unclassified and classified homeland security information to the private sector.

The DHS Secretary's power to prescribe procedures for the dissemination of homeland security information to the private sector is further supported by the **Homeland Security Presidential Directive Number 7 (HSPD 7)**. Paragraph 28 in HSPD 7 states the following:

> The Secretary, consistent with the Homeland Security Act of 2002 and other applicable legal authorities and presidential guidance, shall establish appropriate systems, mechanisms, and procedures to share homeland security information relevant to threats and vulnerabilities in national critical infrastructure and key resources with other Federal departments and agencies, State and local governments, and the private sector in a timely manner.

II. ODNI Authority

The authority given to the DHS Secretary to establish inter-agency procedures for the dissemination of homeland security information to the private sector can easily be confused with the authority given to the ODNI concerning intelligence. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) amended Title 1 of the National Security Act of 1947 to create the ODNI.[67] The ODNI's organizational structure, depicted in Figure 2, provides a foundation from which the DNI can carry out his or her duties and responsibilities under the National Security Act of 1947.[68] According to **Subsection 102(b) of the National Security Act of 1947** (50 U.S.C. § 403(b)), the DNI's principal responsibilities are as follows:

> (1) serve as head of the intelligence community;
> (2) act as the principal adviser to the President, to the National Security Council, and the Homeland Security Council for intelligence matters related to the national security; and
> (3) consistent with section 1018 of the National Security Intelligence Reform Act of 2004, oversee and direct the implementation of the National Intelligence Program.

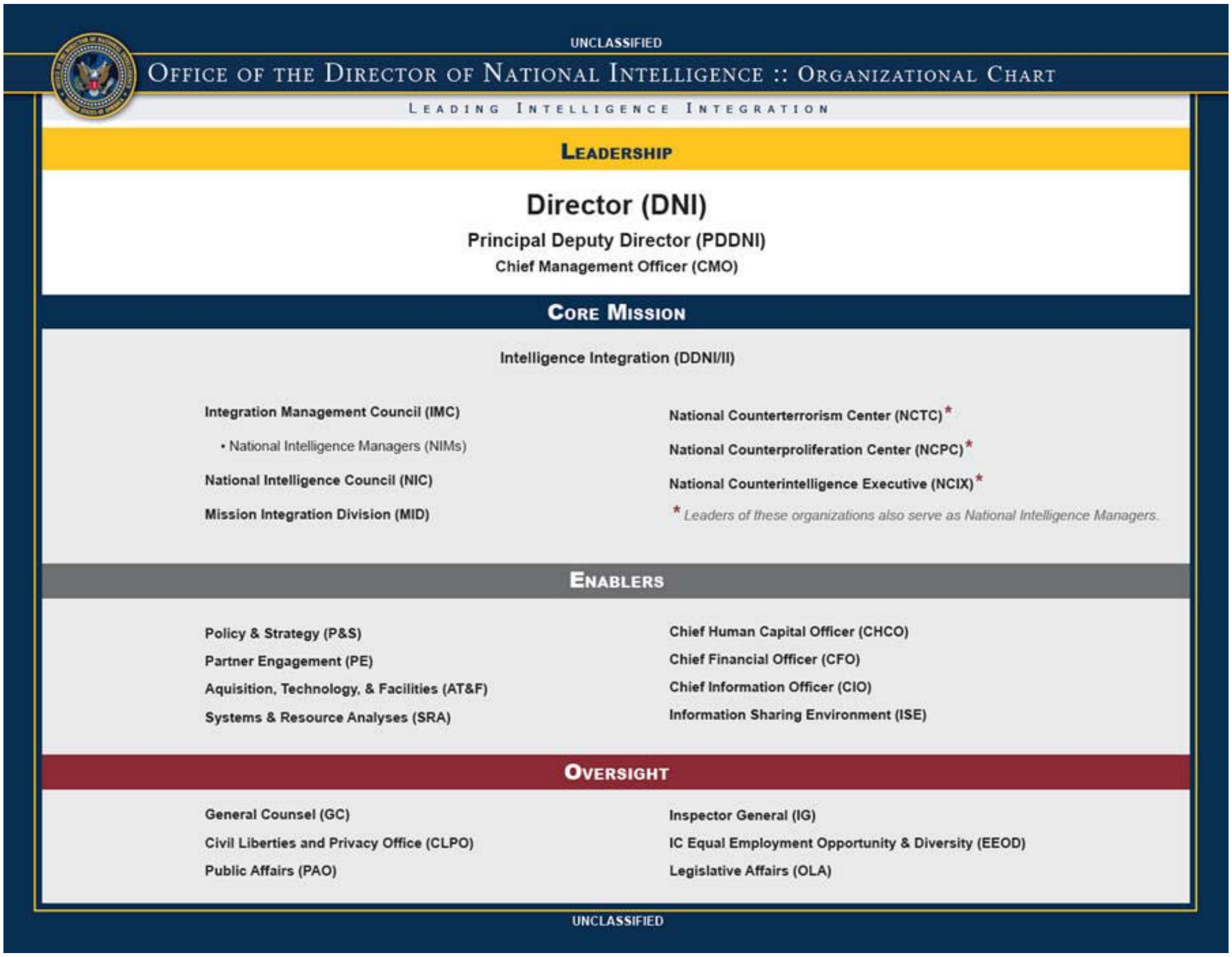
As head of the IC and pursuant to Subsection 102A of the National Security Act of 1947 (50 U.S.C. § 403–1), the DNI shall manage and direct the production and dissemination of national intelligence by the IC's 16 elements depicted in Figure 3. Specifically, the DNI shall --

> **(i)** establish objectives, priorities, and guidance for the intelligence community to ensure timely and effective collection, processing, analysis, and dissemination (including access by users to collected data consistent with applicable law and, as appropriate, the guidelines referred to in subsection (b) of this section and analytic products generated by or within the intelligence community) of national intelligence;
> **(ii)** determine requirements and priorities for, and manage and direct the tasking of, collection, analysis, production, and dissemination of national intelligence by elements of the intelligence community . . .
> **(iii)** provide advisory tasking to intelligence elements of those agencies and departments not within the National Intelligence Program.[69]

[67] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1011, 118 Stat. 3638, 3643-44, 3655 (2004) (codified at 50 U.S.C. § 401, et seq.).
[68] 50 U.S.C. § 403-3(b).
[69] 50 U.S.C. § 403–1(f)(1)(A).

Even though DNI has the range of authority listed above, its ability to share information with the private sector is limited. **Subsection 102A(f)(1)(B)(iii)** (50 U.S.C. § 403–1(f)(1)(B)(iii)) specifically provides that DNI's above listed authority shall not apply to "the direct dissemination of information to State and local government officials and private-sector entities pursuant to sections 121 and 482 of title 6."[70] Consequently, the DHS Secretary's authority to prescribe procedures for Federal agency dissemination of unclassified and classified homeland security information (which would include homeland security related intelligence information) to the private sector remains intact.

Figure 2: ODNI Organizational Chart[71]



UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE :: ORGANIZATIONAL CHART

LEADING INTELLIGENCE INTEGRATION

LEADERSHIP

Director (DNI)

Principal Deputy Director (PDDNI)

Chief Management Officer (CMO)

CORE MISSION

Intelligence Integration (DDNI/II)

Integration Management Council (IMC)

- National Intelligence Managers (NIMs)

National Intelligence Council (NIC)

Mission Integration Division (MID)

National Counterterrorism Center (NCTC)*

National Counterproliferation Center (NCPC)*

National Counterintelligence Executive (NCIX)*

* Leaders of these organizations also serve as National Intelligence Managers.

ENABLERS

Policy & Strategy (P&S)

Partner Engagement (PE)

Aquisition, Technology, & Facilities (AT&F)

Systems & Resource Analyses (SRA)

Chief Human Capital Officer (CHCO)

Chief Financial Officer (CFO)

Chief Information Officer (CIO)

Information Sharing Environment (ISE)

OVERSIGHT

General Counsel (GC)

Civil Liberties and Privacy Office (CLPO)

Public Affairs (PAO)

Inspector General (IG)

IC Equal Employment Opportunity & Diversity (EEOD)

Legislative Affairs (OLA)

UNCLASSIFIED

Figure 3: Intelligence Community Elements[72]

Independent Agency	Central Intelligence Agency

[70] 50 U.S.C. § 403–1(f)(1)(B)(iii).

[71] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Office of the Director of National Intelligence Organization Chart*, http://www.dni.gov/aboutODNI/organization/content/DNIOrgChart.pdf.

[72] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Members of the Intelligence Community*, http://www.dni.gov/members_IC.htm. *See also* 50 U.S.C. § 401a(4).

Offices/Bureaus within Federal Executive Departments	Defense Intelligence Agency	National Reconnaissance Office
	Department of Energy - Office of Intelligence & Counterintelligence	National Security Agency/Central Security Service
	Department of Homeland Security - Office of Intelligence & Analysis	United States Air Force
	Department of State - Bureau of Intelligence & Research	United States Army
	Department of Treasury - Office of Intelligence & Analysis	United States Coast Guard
	Drug Enforcement Administration - Office of National Security Intelligence	United States Marine Corps
	Federal Bureau of Investigation - National Security Branch	United States Navy
	National Geospatial-Intelligence Agency	

III. ISE Overlap

The role of the DHS Secretary to establish inter-agency procedures for sharing unclassified and classified homeland security information with the private sector is even further confused by the creation of the ISE. **Section 1016 of IRTPA**[73] requires that the President (i) create an ISE,[74] (ii) determine and enforce the policies that govern the usage of the ISE,[75] and (iii) ensure that the ISE provides and facilities a mechanism for sharing terrorism information among Federal agencies and private entities.[76] The individual responsible for information sharing across the Federal Government is the program manager (PM).[77] In consultation with the Information Sharing Council,[78] the PM's duties include assisting in the development of policies and procedures that "address and facilitate, as appropriate, information sharing between Federal departments and agencies and the private sector."[79]

Following the enactment of IRTPA, the President issued **Presidential Memorandum of December 16, 2005 (Memorandum).**[80] This Memorandum listed several guidelines to sharing information.[81] Guidelines 1 and 2 are the most relevant to the topics discussed in this Appendix.

Guideline 1 addresses the need to define common standards for how information is shared.[82] It requires that the DNI, in coordination with the Secretaries of State, Defense, and Homeland Security,

[73] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004) (codified at 50 U.S.C. 401, et seq.).
[74] *Id.* § 1016(b)(1)(A).
[75] *Id.* § 1016(b)(1)(C).
[76] *Id.* § 1016(b)(2).
[77] *Id.* § 1016(f)(1).
[78] This refers to the Information Sharing Council established by Executive Order 13,356. The Information Sharing Council assists the President and the program manager in their duties under Section 1016. *Id.* § 1016(g)(1). Specifically, the Information Sharing Council's duties include advising "the President and the program manager in developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE." *Id.* § 1016(g)(2).
[79] *Id.* § 1016(f)(2)(B)(vi).
[80] Memorandum from the President for the Heads of Executive Departments and Agencies, Subject: Guidelines and Requirements in Support of the Information Sharing Environment (Dec. 16, 2005).
[81] Presidential Memorandum, Guidelines and Requirements in Support of the Information Sharing Environment (Dec. 16, 2005).

and the Attorney General, develop and issue common standards to enable the sharing of terrorism information within the ISE.[83] Such standards are required to "accommodate and reflect" the sharing of information with the private sector.[84] The authority to later amend the common standards is given to the DNI.[85]

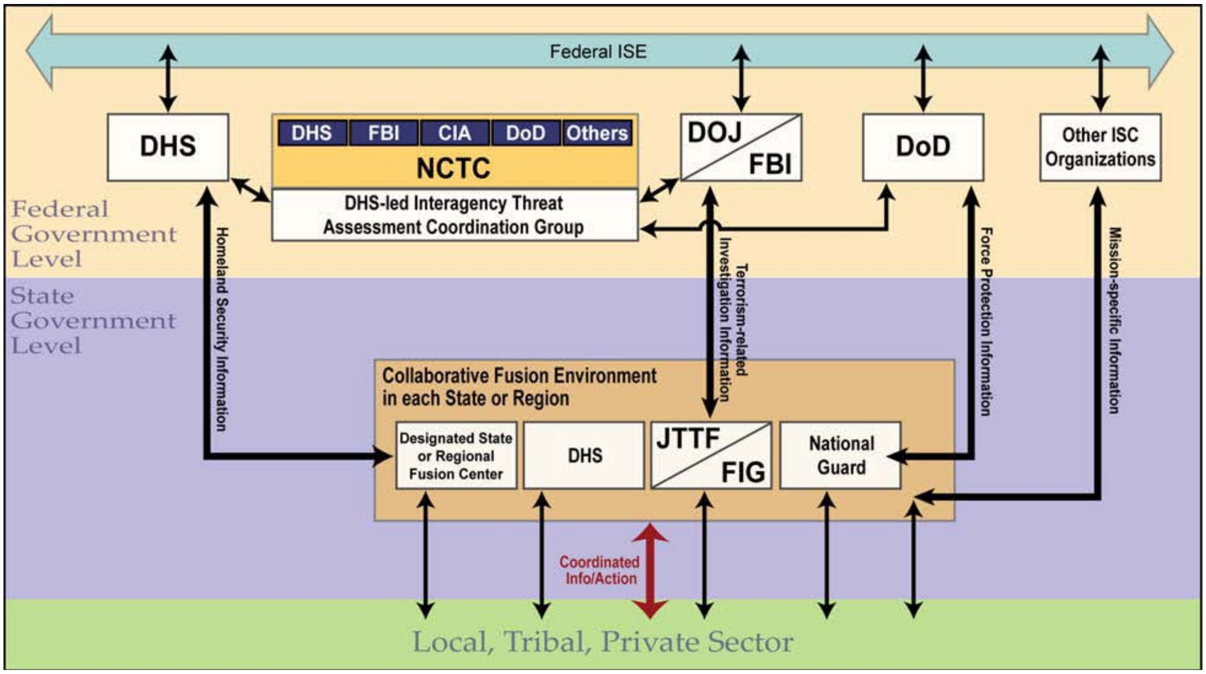
Guideline 2 addresses developing a common framework for sharing information between and among Federal agencies and the private sector.[86] The DHS Secretary and the Attorney General, in consultation with the Secretaries of State, Defense, and Health and Human Services, and the DNI, are responsible for "submit[ing] to the President for approval . . . a recommended framework to govern the roles and responsibilities of executive departments and agencies pertaining to the . . . sharing of homeland security information, law enforcement information, and terrorism information between and among such departments and agencies . . . and private sector organizations."[87]

The **ISE Implementation Plan (Plan)** builds off IRTPA and the Memorandum. Per IRTPA, the Plan is to include the policies and directives referred to in Subsection 1016(b) (1) (C). It is also required to include the delineation of the roles of the Federal agencies that are to participate in the ISE, with such role delineation to be consistent with the authority of the DHS Secretary in coordinating with the private sector.[88]

According to the Plan, "the Attorney General and the Secretary of Homeland Security, in consultation with the PM-ISE, the ISC, and Federal departments and agencies . . . established a Presidentially-approved framework (pursuant to Presidential Guideline 2) through which terrorism information can be shared in a distributed, decentralized, and coordinated manner between and among participating Federal, SLT, and private sector entities."[89] Under the established framework, depicted in Figure 4, the roles and responsibilities of participating Federal agencies are meant to be preserved.[90] The framework mandates, however, a "coordinated and collaborative approach to sharing information with . . . the private sector."[91] Specifically, Federal agencies assigned mission-specific roles are to provide terrorism information to the Interagency Threat Assessment and Coordination Group (ITACG).[92] ITACG is then responsible for "facilitat[ing] the production of 'federally coordinated' terrorism information products intended for dissemination to State, local and tribal officials and private sector partners."[93] Decision-making authority concerning how information will be disseminated to the private sector, however, is to "be primarily shared between DHS and DOJ and will include other agencies as appropriate."[94] Therefore, DHS does have authority and responsibility for establishing how terrorism information is to be disseminated to the private sector. DOJ, however, appears to have overlapping authority on the matter.

[82] *Id.* § 2(a).
[83] Id.
[84] Id.
[85] *Id.* "The DNI may amend the common standards from time to time as appropriate through the same process by which the DNI issued them." *Id.*
[86] *Id.* § 2(b).
[87] *Id.* § 2(b)(ii).
[88] *Id.* §§ 1016(e)(5), (10).
[89] Information Sharing Environment Implementation Plan xix (Nov. 2006).
[90] *Id.* at 72.
[91] *Id.*
[92] *Id.* at 28.
[93] *Id.* at 29. Mission-specific information is to be disseminated according to established. *Id.*
[94] *Id.*

Figure 4: Approved Guideline 2 Framework[95]


Federal ISE
DHS
DHS
FBI
CIA
DoD
Others
NCTC
DHS-led Interagency Threat Assessment Coordination Group
DOJ
FBI
DoD
Other ISC Organizations
Federal Government Level
State Government Level
Homeland Security Information
Terrorism-related Investigation Information
Force Protection Information
Mission-specific Information
Collaborative Fusion Environment in each State or Region
Designated State or Regional Fusion Center
DHS
JTTF
FIG
National Guard
Coordinated Info/Action
Local, Tribal, Private Sector

Conclusion

The laws and policies referenced in this Appendix create somewhat of an authority overlap with regard to establishing inter-agency procedures for the dissemination of intelligence and homeland security information to the private sector. Despite confusion resulting from this authority overlap, it is clear that: 1) the Homeland Security Act and EO 13,311 expressly provide the DHS Secretary with the authority to establish such procedures with regards to unclassified and classified homeland security information, and 2) the National Security Act of 1947 expressly provides that the DNI does not have authority over direct dissemination of information to private sector entities pursuant to the Homeland Security Act.

[95] *Id.* at 71.

Appendix I. The Federal Structure for Intelligence Information Sharing

The sharing of intelligence between government and critical infrastructure owners and operators is an exceedingly complex subject and a goal not easily defined or achieved. This section discusses key elements of this challenge, including the structure of the Intelligence Community (IC); the missions of the various IC components; key definitions such as “national intelligence, “homeland security information,” and “terrorism information”; the evolution to the all-hazards threat environment of today; illustrative models of information sharing with the private sector; and some issues of concern in the sharing of intelligence with the private sector.

Components of the Federal Intelligence Community

The Intelligence Community (IC) is defined at 50 U.S.C. 401a (4) as consisting of the following organizations, each of which has legally prescribed roles and responsibilities (See Figure 1). The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) created the Director of National Intelligence, who heads the Intelligence Community, advises the President on intelligence matters, and – among other things – is charged with establishing priorities for budgets, directing collection, and preparing community-wide analytical products.[96]

Figure 1. Components of the U.S. Intelligence Community

IC Component	Primary Mission Area
Independent Agency	
Central Intelligence Agency (CIA)	Independent agency and separate program with all-source analytical capabilities that cover the entire world outside U.S. borders; produces studies addressing any topic of interest to national security policymakers; responsible for human intelligence and covert action at the direction of the President.
DOD Intelligence Components	
National Security Agency (NSA)	National-level agency and program in Department of Defense (DOD); responsible for signals intelligence with collection sites throughout the world.
National Reconnaissance Office (NRO)	National-level agency and program in DOD responsible for developing and operating reconnaissance satellites.
National Geospatial-Intelligence Agency (NGA)	National-level agency and program in DOD responsible for preparing geospatial data necessary for targeting.
Defense Intelligence Agency (DIA)	Program and component in DOD responsible for defense attachés and providing DOD with analytical products. (Continued)

[96] For an overall description of the U.S. Intelligence Community, see Richard A. Best, Jr., “Intelligence Issues for Congress,” Congressional Research Service Report RL33539, August 5, 2011, http://www.fas.org/sgp/crs/intel/RL33539.pdf. For an overview of the Office of the Director of National Intelligence and the Intelligence Community, see ODNI, *National Intelligence: a consumer’s guide – 2009*, http://www.dni.gov/IC_Consumers_Guide_2009.pdf.

Figure 1. Components of the U.S. Intelligence Community (Continued)

IC Component	Primary Mission Area
Army Intelligence, Navy Intelligence, Air Force Intelligence, and Marine Corps Intelligence	Separate service intelligence components responsible for supporting their specific military service, and providing depth of analysis on military and technical issues for DIA and CIA. The U.S. Coast Guard is also a service intelligence component, now part of DHS (see below).
Departmental Intelligence Components	
Bureau of Intelligence and Research (INR)	State Department component responsible for analyzing intelligence about foreign countries acquired through U.S. embassies and other sources.
Federal Bureau of Investigation (FBI), National Security Branch	Department of Justice component and program responsible for counterterrorism and counterintelligence; forwarding law enforcement information to other intelligence agencies for use in all-source products.
Office of Intelligence & Counterintelligence	Department of Energy component responsible for analyzing foreign nuclear weapons programs, as well as nuclear nonproliferation and energy-security issues.
Office of Intelligence & Analysis	Department of Treasury component responsible for collecting and processing information that may affect U.S. fiscal and monetary policies, as well as terrorist financing issues.
United States Coast Guard	Part of DHS but considered separate member of IC, responsible for intelligence relating to maritime security and homeland defense.
Office of National Security Intelligence	Part of the Drug Enforcement Administration, within the Department of Justice, responsible for intelligence related to illicit drugs entering the U.S., including interdiction cooperation with foreign countries.
Office of Intelligence & Analysis	Department of Homeland Security component responsible for fusing law enforcement and intelligence information relating to terrorist threats to the homeland; focuses, in cooperation with FBI, on ensuring that State and local law enforcement officials receive information on intelligence threats from national-level intelligence agencies.
Organizations with a Close Relationship to the Intelligence Community	
Joint Terrorism Task Forces (JTTFs)	FBI-led multi-organizational task forces composed of local, State, and Federal entities; found in over 100 cities nationwide; coordinated by National Joint Terrorism Task Force in Washington, D.C.
Fusion Centers	Combine resources at State, local, and tribal levels to improve detection and response to crimes and terrorism; over 70 nationwide, including all 50 States and the District of Columbia; capabilities vary, but most include State and local law enforcement, public health and safety entities, and Federal entities such as the FBI, DHS, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF).

As discussed more fully in Appendix H (DHS Authorities in Intelligence Information Sharing), the Director of National Intelligence (DNI), as head of the IC and pursuant to Subsection 102A of the National Security Act of 1947 (50 U.S.C. § 403-1), has the authority to "establish objectives, priorities, and guidance for the intelligence community to ensure timely and effective collection, processing, analysis, and dissemination…of **national intelligence** by elements of the intelligence community." The Secretary of Homeland Security, pursuant to the Homeland Security Act (HSA) of 2002 (6 U.S.C. § 482) and Executive Order 13311 of 2003, has the authority to establish procedures for the dissemination of **homeland security information** – both classified and unclassified – to the private-sector owners and operators of critical infrastructure. [emphasis added]

Defining Intelligence Information

There is a difference between "national intelligence" and "homeland security information." **National intelligence** refers to information, regardless of its source, that involves threats to U.S. persons, property, or interests, including weapons of mass destruction or matters "bearing on United States national or homeland security." (50 U.S.C. § 401a (5) (2006)). **Homeland security information,** as defined by the HSA, applies specifically to information possessed by Federal, State, or local agencies that relates to **terrorist activity**. (6 U.S.C. § 482(f) (1) (2006))

Terrorism information is defined in the HSA as "all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security or other activities" relating to international and domestic terrorist groups or individuals, threats posed by such groups or individuals to the U.S., its persons or interests or those of other nations, and weapons of mass destruction. (6 U.S.C. § 485(a) (5)) Hence, information related to terrorism, whether collected domestically or internationally and from any source, is included in the definitions of both homeland security information and intelligence information. In the period immediately following 9-11, the focus of public-private intelligence/information sharing was terrorist-related.

All-Hazards

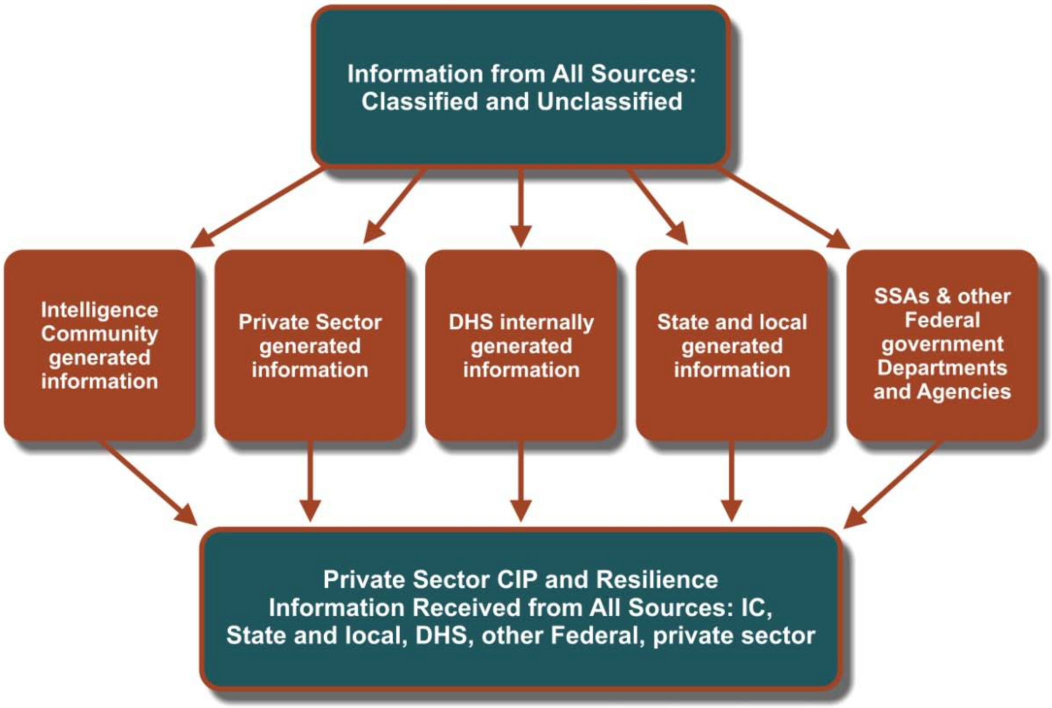
In the aftermath of Hurricane Katrina in 2005, homeland security information was broadened to include not only terrorist threats to critical infrastructure but also natural threats such as hurricanes and pandemics. Also, other kinds of manmade threats were added to the category of homeland security information, such as threats posed by disgruntled employees and criminal activities such as theft of copper from electricity sub-stations. Over the past few years, homeland security information has been expanded further to include cyber threats such as unauthorized control of SCADA systems used in many elements of the nation's critical infrastructure. Homeland security information in the current threat environment is based on threats from "all-hazards." DHS is responsible for the dissemination of all-hazards homeland security information to Federal, State, and local governments and to the private sector.

Part of the intelligence generated by the IC relates to the all-hazards homeland security needs of DHS and its stakeholders at the State and local government and private-sector levels. Other types of intelligence do not relate to homeland security. In order to receive the specific kind of intelligence needed by the private sector, whether classified or unclassified, the Office of the DNI (ODNI) must establish requirements and tasking for the collection, analysis, production, and dissemination of such information by elements of the IC. In order for the intelligence to reach critical infrastructure stakeholders, DHS must establish appropriate information-sharing mechanisms and products. Neither the ODNI nor the DHS – nor any other single component of government – can on its own provide 18 critical infrastructure sectors with the kinds of intelligence information they require for protection and resilience against current threats.

The Flow of Intelligence Information

The flow of information to the private sector is illustrated in Figure 2. All agencies of the U.S. government, all components of State and local governments, and all private-sector entities are legitimate providers of critical infrastructure protection and resilience information to the CIKR owners and operators. However, DHS has special responsibility for homeland security information dissemination, and the ODNI has special responsibility in ensuring that the Intelligence Community collects, analyzes, produces, and disseminates national intelligence that supports the homeland security mission.

Figure 2. Information Flow to Private Sector


Information from All Sources: Classified and Unclassified
Intelligence Community generated information
Private Sector generated information
DHS internally generated information
State and local generated information
SSAs & other Federal government Departments and Agencies
Private Sector CIP and Resilience Information Received from All Sources: IC, State and local, DHS, other Federal, private sector

Because there are overlaps of definitions and responsibilities, there has to be both a **systemic improvement** in intelligence sharing between the IC, DHS, and the private sector (mostly under the auspices of the ODNI or the White House), as well as a **process improvement** whereby DHS and/or the private sector enter into special arrangements (often through such mechanisms as memorandum of understanding or protocols) with components of the IC. Figure 3 illustrates this latter approach.

National Information Sharing Environment (ISE)

A common theme following the terrorist attacks of 2001 was the need to share timely and actionable information on terrorism-related matters with a variety of agencies across all levels of the government. The Intellgience Reform and Terrorism Prevention Act (IRTPA) mandated that the President create the Information Sharing Environment (ISE), which is an approach for sharing terrorism-related information that may include any method determined necessary and approprate. The President designated a Program Manager for the ISE (PM-ISE) to plan for, oversee implementation of, and manage the ISE. The ISE provides the approprate government personnel with integrated and synthesized terrorism, weapons of mass destruction, and homeland security information needed to enhance national security and help keep americans safe.[97]

The ISE is intended to be a decentralized and coordinated environment that builds upon existing systems and leverages ongoing efforts. The ISE leverages the personnel of five Federal communities—defense, foreign affairs, homeland security, intelligence, and law enforcement—along with infrastructure owners/operators and Federal, State, local, tribal, and territorial governments. Given this diversity of mission partners, the role of the PM-ISE is to bring ISE mission partners together to collaborate and support shared, cross-organizational solutions based on collective mission equities, to

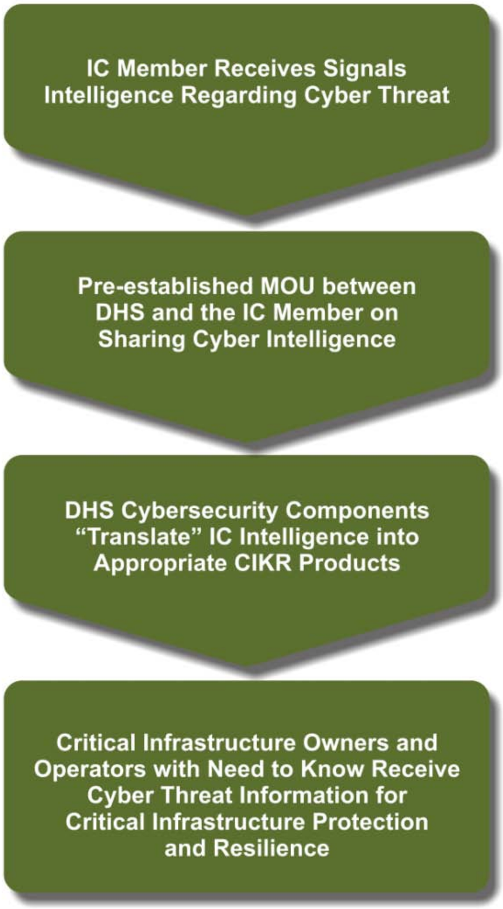
[97] "Information Sharing Environment," web page, 2011. http://www.ise.gov/what-ise

build consensus to prioritize funding and deliver on a shared vision, and to provide a collective management and governance framework to accelerate nationwide results.

Since the Congressional call for the creation of the ISE, progress has been made within the ISE to develop a foundation for information sharing across the Federal Government. The ISE has met preliminary goals for sharing terrorism, weapons of mass destruction, and homeland security information.[98] The following are key ISE intiatives:

- *Nationwide Suspicious Activity Reporting Initiative (NSI)*: The NSI establishes a national capacity for gathering, documenting, processing, analyzing, and sharing Suspicious Activity Reports (SARs).
- *Fusion Center Baseline Capabilities Assessment*: Federal, State, and local officials launched the 2010 Baseline Capabilities Assessment (BCA) in April 2010 in the first formal attempt to gauge fusion centers' capabilties. Federal partners are leveraging the BCA results to work with fusion centers to mitigate existing gaps in fusion centers' capabilities.[99]
- *Development of Common Standards and Shared Approaches*: Mission partners within the ISE are accelerating the development and approval of common standards and practices for usage across the ISE.
- *CIKR Information Sharing Environment*: In 2007, the CIKR ISE was adopted as a component of the ISE for focused implementation.

Figure 3. Process for Information Flow from IC to Private Sector (Illustrative)


IC Member Receives Signals Intelligence Regarding Cyber Threat
Pre-established MOU between DHS and the IC Member on Sharing Cyber Intelligence
DHS Cybersecurity Components "Translate" IC Intelligence into Appropriate CIKR Products
Critical Infrastructure Owners and Operators with Need to Know Receive Cyber Threat Information for Critical Infrastructure Protection and Resilience

Despite these accomplishments recent evalautions convey that ISE is far from fully-functioning. A July 2011 Government Accountability Office (GAO) Report built upon previous GAO examination of the ISE notes that the ISE lacks a clear roadmap to guide its implementation and budget. Activities such as the NSI do not fully address GAO recommendations or provide a comprehensive roadmap. This roadmap, according to the GAO, should identify the key next steps for ISE development and start with a clear definition of what the ISE is intended to achieve and include—or the "end state" vision. The report also found that the PM-ISE and affected agencies have not yet identified the incremental costs necessary to implement the ISE—which would allow decision makers to plan for and prioritize future investments.[100]

[98] Program Manager for the Information Sharing Environment, ISE Annual Report to Congress, June 2011, http://www.ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2011.pdf

[99] Department of Homeland Security, "Critical Operational Capabilities for State and Major Urban Area Fusion Centers: Gap Mitigation Strategy." December 2010.

[100] Government Accountability Office, *Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investments*. July 2011. http://www.gao.gov/new.items/d11455.pdf

Challenges in Intelligence Information Sharing

There are several important issues that need to be addressed in the sharing of intelligence information between the Intelligence Community and the private sector. These include missions, the ownership of intelligence information, sources of information, analytical capability, collection requirements, stovepiping, and the protection of privacy and civil liberties. Effective resolution of these issues will require a concerted, coordinated effort among public and private-sector partners. These issues were cited repeatedly in the case studies and are discussed briefly below.

Missions

The primary consumer of national intelligence is the Federal Government, which uses the information to improve and understand the consequences of its national security decisions. The intelligence also informs policy, military actions, international negotiations, and interaction with contacts in foreign countries. The use of national intelligence by critical infrastructure owners and operators (most of whom are domestically based in the United States and few of whom have security clearances) requires a deliberate, yet timely process of divorcing highly-sensitive sources and methods information from the "actionable" information needed by critical infrastructure to ensure their protection and resilience in an all-hazards environment. As shown in Figure 2, there is no IC component tasked with the single mission of collecting, analyzing, and disseminating intelligence for use by the critical infrastructure community. DHS I&A has responsibilities in this area (in addition to border security, chemical/biological/ radiological/nuclear issues, extremists in the U.S., and travelers entering the U.S.), but it is not considered a major "collector" of national intelligence.

Ownership of Information

Within the IC, the collector of the intelligence is the "owner" of the intelligence; i.e., the entity responsible for determining and authorizing the dissemination of the intelligence. This is done to protect sensitive sources and methods, but it results in a twofold hurdle for IC components such as DHS, DOE, Treasury, or the FBI that may want to pass on the intelligence to their private-sector partners. These hurdles are (1) the decision to release the information resides with the owner; and (2) the owner has the right to review, modify, or hold indefinitely the redacted version of the original intelligence. Unless procedures are in place to expedite the processing of national intelligence into digestable formats approved for dissemination to State and local officials and/or the private sector, the securing of the owner's approval on a particular piece of intelligence can take so long as to negate the timeliness and actionability of the intelligence. This is one of the main reasons the private sector complains frequently and loudly about the timeliness of threat information received from the Federal Government.

Sources of Information

There are three broad categories of information produced and used by the IC and the private-sector owners and operators of critical infrastructure: classified information (as determined by Executive Order 13529 of December 29, 2009,[101] or the Atomic Energy Act, as amended), controlled unclassified information (as determined by Executive Order 13556 of November 4, 2010[102]), and open-source

[101] See, Executive Order 13526—Classified National Security Information; Memorandum of December 29, 2009—Implementation of the Executive Order ''Classified National Security Information'' Order of December 29, 2009—Original Classification Authority, http://edocket.access.gpo.gov/2010/pdf/E9-31418.pdf.

[102] See, Executive Order 13556 of November 4, 2010, "Controlled Unclassified Information," http://edocket.access.gpo.gov/2010/2010-28360.htm.

Balancing Law Enforcement and Critical Infrastructure Protection Missions:
The Issue of Continuing Harm

While a clear and growing concern is the compromise of business-critical information from cyber intrusions, an underlying concern is the potential for continuing harm after an intrusion is first discovered. This can occur when the law-enforcement's desire to learn more about the perpetrator(s) lets the intrusion continue. One example was described by the Chairperson of the FSSCC in testimony before Congress on April 15, 2011.* The incident she described was an intrusion through the Directors Desk web-facing service at NASDAQ OMX Group.** She said:

"An example of an incident where too much secrecy led to an increased exposure was the cyber attack on a major exchange, which was discovered by the exchange in October 2010. The exchange alerted its primary regulator and law enforcement. For a variety of reasons, including an investigation of the attack by law enforcement and intelligence agencies, information about the attack and its impact on other financial institutions was not disclosed to others in the financial services sector for 102 days. This 102-day period included year-end, when financial institutions close their books and prepare annual reports. This could have had an enormous impact on employees, stockholders large and small, and the market as a whole. The lack of meaningful information for more than three months left the entire Sector unnecessarily vulnerable."

Sources:

* Jane Carlin, before the Subcommittee on Cyber Security, Infrastructure Protection and Security Technologies of the Homeland Security Committee of the House of Representatives, April 15, 2011.

** Devlin Barrett, "Nasdaq Acknowledges Security Breach," online WSJ, February 6, 2011, http://online.wsj.com/article/SB10001424052748704843304576126370179332758.html.

information (which can be loosely defined as information from publicly available sources[103]). Sensitive or proprietary information produced and used by the private sector generally falls into the controlled unclassified information category of the Federal Government.

There is an increasing trend both within government and within the private sector to use open-source information. This information, much of which is freely available on the Internet, can be categorized and analyzed to produce actionable intelligence, such as discerning patterns of behavior likely to be predictive of future terrorist or criminal activity.

In the all-hazards threat environment of critical infrastructure owners and operators, controlled unclassified information and open-source information are the most valuable sources of intelligence, although owners and operators look to the Intelligence Community to provide them with specific threat information not otherwise available to the private sector. The private sector, in turn, possesses unclassified information that can be of great value to the IC, such as reports on suspicious activities near their facilities or evidence of radicalization of employees.

Moreover, with the emergence of national-level threats from cyberspace, there is a growing recognition within both government and the private sector that intelligence and information flows must be bidirectional, if public-private interests in a secure critical infrastructure are to be served.

Analytical Capability

The homeland security, critical infrastructure protection mission is relatively new for the IC, most components of which focused for decades on threats associated with the Soviet bloc. There are

[103] "Open source intelligence" is the finding and analysis of open source information to produce actionable intelligence. See, https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html.

relatively few critical-infrastructure analysts within the IC, and most analysts who have gained some expertise in one or more of the critical infrastructure sectors have done so “on the job” or brought experience from previous employment. Intelligence analysts who do not understand critical infrastructure may not always know that they are examining an important piece of information that would be valuable to an owner or operator in one of the CIKR sectors.

Requirements for Critical Infrastructure Intelligence Collection

Another issue centers around the National Intelligence Priorities Framework (NIPF) process, whereby the ODNI establishes national-intelligence priorities against which IC components measure their collection requirements and analytic production. Without a strong advocate, the intelligence requirements of the critical infrastructure community tend to move down the list of priorities, especially during a period of multiple overseas conflicts and escalating cyber intrusions, some of which may originate from state-sponsored activities.

Stovepiping

There is also the perrenial issue of intelligence agencies being reluctant to share their information with others in the IC out of a concern to protect their sources. There is a continuous tug-of-war between advocates of “need to share” and “need to know” in the IC, and the unauthorized disclosure of classified documents through Wikileaks has reinforced the tendency within government intelligence and law-enforcement communities to limit the sharing of information with the private sector.

Civil Liberties and Privacy

The IC and the law-enforcement community are especially concerned with protecting privacy and civil liberties. The collecting of information about U.S. persons and the sharing of that information – even within government – is highly sensitive and carefully monitored to ensure compliance with strict laws and regulations. This hightened sensitivity can work against the sharing of intelligence information relevant to the critical infrastructure community, as in the case of suspicious activity reports that identify a particular person or group as a potential threat to a given facility.

Appendix J. The DHS Structure for Infrastructure Protection

This appendix is presented in two parts. The first addresses the DHS organization for infrastructure protection and the second addresses mechanisms used to promote information sharing.

1.0 Organization

Two of the most important organizations within DHS for the purpose of infrastructure protection are the Office of Intelligence and Analysis (I&A) and the Office of Infrastructure Protection (IP). The Office of Intelligence and Analysis is headed by an Under Secretary. The Office of Infrastructure Protection is headed by an Assistant Secretary; IP is part of the National Protection and Programs Directorate (NPPD), led by an Under Secretary.

Originally, I&A and IP were part of a single organization within DHS, the Directorate for Information Analysis and Infrastructure Protection (IAIP). Section 201 of the Homeland Security Act (HSA) of 2002 established IAIP, to be headed by an Under Secretary for Information Analysis and Infrastructure Protection. The Under Secretary was to be assisted by a presidentially appointed Assistant Secretary for Information Analysis and an Assistant Secretary for Infrastructure Protection. Sections 872 and 1502 of the HSA authorized the Secretary of Homeland Security and the President, respectively, to reorganize DHS within certain limits. President George W. Bush and Secretary Michael Chertoff exercised this authority in ways that led to the division of IAIP in 2005.[104]

Briefly, what occurred was that the passage of the Intelligence Reform and Terrorism Prevention Act of 2004, and the creation of the National Counter Terrorism Center (NCTC) and the Terrorist Screening Center (TSC) prompted both the Senate and the House to direct DHS to reconsider the role and mission of IAIP in the intelligence community.

On July 13, 2005, Secretary Chertoff sent to Congress a reorganization notification letter in which he stated that the Information Analysis component of IAIP would be elevated to a stand-alone Office of Intelligence and Analysis (IA), headed by the Assistant Secretary for Information Analysis (re-titled as Chief Intelligence Officer), reporting directly to the Secretary.[105] Stating that DHS was an all-hazards department, the Secretary consolidated the Department's prevention, protection, response, and recovery functions into a new Preparedness Directorate, headed by the Under Secretary for Preparedness.[106]

Subsequently, the Safe Port Act of 2006 elevated the position of Assistant Secretary of I&A to an Under Secretary level. The Implementation of the Post-Katrina Emergency Management Reform Act and other organizational changes in early 2007 renamed the Preparedness Directorate to the National Protection and Programs Directorate (NPPD), continued to be led by an Under Secretary. This organizational structure remains in place today.

[104] The background to the division of IAIP can be found in CRS Report to Congress RL33042, "Department of Homeland Security Reorganization: The 2SR Initiative," updated September 22, 2006, available at: http://digital.library.unt.edu/ark:/67531/metacrs9942/.

[105] Ibid., p. CRS-7.

[106] Ibid., pp. CRS-9-11.

Office of Intelligence and Analysis (I&A)

The current Under Secretary of I&A – who is also the Department's Chief Intelligence Officer – recently noted the complexity of the I&A mission in testimony before the House Intelligence Committee on Homeland Security:[107]

> "DHS is a complex organization with a broad, diverse set of missions. Intelligence is an important supporting factor in most, if not all, of these missions. Departmental intelligence programs, projects, activities, and personnel – including the intelligence elements of our seven key operational components, as well as the Office of Intelligence and Analysis (I&A) – make up the DHS Intelligence Enterprise (IE). I&A is charged with ensuring that intelligence from the DHS IE is analyzed, fused, and coordinated to support the full range of DHS missions and functions, as well as the Department's external partners. The operational components, most of which predate the creation of the Department, have intelligence elements that provide support tailored to their specialized functions and contribute information and expertise in support of the Department's broader mission set."

Figure 1. Members of the DHS Intelligence Enterprise

Members of the DHS Intelligence Enterprise include:

- I&A (Intelligence analysts from several components)
- Immigration and Customs Enforcement (Office of Intelligence)
- U.S. Citizenship and Immigration Services (Fraud Detection and National Security)
- Transportation Security Administration (Office of Intelligence)
- Customs and Border Protection (Office of Intelligence & Operations Coordination)
- Federal Emergency Management Agency (National Preparedness Directorate)
- National Protection and Programs Directorate (Office of Infrastructure Protection)
- U.S. Secret Service (Protective Intelligence & Assessment Division)
- Office of the Chief Security Officer (Chief Security Officer)
- U.S. Coast Guard (Intelligence & Criminal Investigation)
- Operations (Director of Operators Coordination)
- State & Local Program Office (Director, Joint Fusion Center)

The members of the DHS Intelligence Enterprise are listed in Figure 1.[108] Of these DHS IE components, only I&A and the U.S. Coast Guard are members of the U.S. Intelligence Community. The I&A Strategic Plan for FY 2011-2018 specifies that the Office serves the intelligence needs of five key customers or "partners":[109]

- Departmental leaders
- State, Local, Tribal, and Territorial Partners
- DHS Component Operators
- Intelligence Community Members
- Private Sector

[107] Statement for the Record of Caryn A. Wagner, Under Secretary and Chief Intelligence Officer, Office of Intelligence and Analysis, before the Subcommittee on Counterterrorism and Intelligence House Committee on Homeland Security, "The DHS Intelligence Enterprise - Past, Present, and Future," June 1, 2011, http://www.dhs.gov/ynews/testimony/testimony_1306937528609.shtm.

[108] For a description of the DHS IE, see CRS, "The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress," R40602, May 27, 2009, http://epic.org/crs-rept_dhs-oversight.pdf.

[109] See, DHS, Office of Intelligence and Analysis, *Strategic Plan, Fiscal Year 2011 – Fiscal Year 2018*, February 2011, http://www.dhs.gov/xlibrary/assets/ia-fy2011-fy2018-strategic-plan.pdf. The Strategic Plan also explains I&A's mission, strategic goals, and objectives, several of which address some of the concerns raised during the course of the current NIAC study. See pages 7-18.

It is important to note that the I&A Under Secretary is concurrently the Chief Intelligence Officer (CINT) of DHS. The CINT is "responsible for leading and managing the activities of the DHS IE, and furthering a unified, coordinated, and integrated intelligence program for the Department."[110] All heads of DHS intelligence components are required by law (Implementing Recommendations of the 9/11 Commission Act of 2007) to advise and coordinate with – but not report to – the CINT. This coordination primarily occurs through the Homeland Security Intelligence Council (HSIC), which serves as the DHS IE decision-making and implementation oversight body. Among its other functions, HSIC creates working groups as needed to address the requirements of the DHS IE.

Of the various elements of I&A, among the most important in terms of this current NIAC study are the State and Local Program Office; the Cyber, Infrastructure, and Science Division; and the Private Sector Partnership Program. The role of these activities in the sharing of intelligence information with the private sector is discussed in the Findings section of this report.

Office of Infrastructure Protection (IP)

Originally part of IAIP, the Office of Infrastructure Protection now resides within the National Protection and Programs Directorate (NPPD). Unlike I&A, whose responsibilities encompass the intelligence needs of the entire Department of Homeland Security, NPPD/IP focuses almost exclusively on the protection and resilience of critical infrastructure.

NPPD/IP leads the coordinated national program to (1) reduce risks to the nation's critical infrastructure posed by acts of terrorism, and (2) strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.[111] NPPD/IP supports the implementation of the *National Infrastructure Protection Plan* (NIPP) (http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf) through a broad set of programs and activities designed to support critical infrastructure partners in the field. Working in collaboration with Federal, State, local, tribal, territorial, international, and private-sector partners to strengthen the protection and resilience of the nation's critical infrastructure, NPPD/IP utilizes the NIPP sector partnership structure and risk management framework to identify assets, systems, networks, and functions whose loss or compromise pose the greatest risk to homeland security. NPPD/IP is also the Sector-Specific Agency (SSA) of six of the 18 critical infrastructures.

The several Divisions of NPPD/IP are shown in Figure 2. The considerable resources offered by NPPD/IP and other elements of DHS to the private sector to assist in critical infrastructure protection and resilience are compiled in the DHS publication, *Private Sector Resources Catalog*, the latest version of which was published in July 2011.[112]

Homeland Infrastructure Threat and Risk Analysis Center

The Congress, in Section 201 of the Homeland Security Act of 2002,[113] placed under one administrative umbrella the combined capabilities of DHS intelligence and DHS critical infrastructure expertise. Section 201 (d), paragraphs 1-19, of the Act lists the responsibilities of the Under Secretary of IAIP, several of which are shown in Figure 3.

[110] Statement of Caryn A. Wagner, before the Subcommittee on Counterterrorism and Intelligence House Committee on Homeland Security, "The DHS Intelligence Enterprise - Past, Present, and Future," June 1, 2011, http://www.dhs.gov/ynews/testimony/testimony_1306937528609.shtm.

[111] See DHS IP home page at http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm.

[112] *Private Sector Resources Catalog*, version 3.0, July 2011, DHS Private Sector Office, http://www.dhs.gov/xlibrary/assets/pso-private-sector-resource-catalog-3.pdf.

[113] See, Homeland Security Act of 2002, http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.

Figure 2. Divisions in the Office of Infrastructure Protection

Contingency Planning and Incident Management Division. CPIMD plans and coordinates critical infrastructure-focused response to natural disasters and manmade incidents. CPIMD operates the National Infrastructure Coordinating Center, one of five elements of the DHS National Operations Center.

Infrastructure Analysis and Strategy Division. IASD focuses on critical infrastructure-related modeling, simulation, and analysis. IASD maintains the Homeland Security Infrastructure Threat and Risk Analysis Center (HITRAC), and the National Infrastructure Simulation and Analysis Center (NISAC).

Infrastructure Information Collection Division. IICD acquires infrastructure data and provides it in standardized formats to public and private-sector homeland security partners to enhance planning and emergency response.

Infrastructure Security Compliance Division. ISCD leads national implementation of the Chemical Facility Anti-Terrorism Standards (CFATS). The CFATS program assesses high-risk chemical facilities, promotes collaborative security planning, and ensures that covered facilities meet risk-based performance standards.

Partnership and Outreach Division. POD develops and sustains strategic partnerships and information sharing with owners and operators of the nation's critical infrastructure and provides outreach and training support to assist State, tribal, and local homeland security partners.

Protective Security Coordination Division. PSCD reduces risk to the nation's critical infrastructure and key resources through site-vulnerability assessments, Protective Security Advisors, the Regional Resiliency Assessment Program, and the Office of Bombing Prevention.

Sector-Specific Agency Executive Management Office. SSA EMO oversees critical infrastructure protection in six of the 18 critical infrastructure sectors — Chemical; Commercial Facilities; Critical Manufacturing; Dams; Emergency Services; and Nuclear Reactors, Materials, and Waste.

As IAIP developed, it was determined that a single organization within the Directorate could best integrate intelligence and critical-infrastructure expertise: the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC).

HITRAC was established in January 2005 to assess risks to domestic critical infrastructure and key resources (CIKR) through integration of intelligence reporting and analysis with information from infrastructure sectors. Its purpose was to be a center for intelligence analysis and risk assessment devoted to protecting and securing the homeland. As explained to Congress by the Acting Director of HITRAC in November 2005:[114]

> "HITRAC is meant to institutionalize risk assessments, as well as to produce some tailored threat assessments that can support the protection of the national critical infrastructure and our key resources. HITRAC reports both to the Office of Intelligence and Analysis, as well as to the Office of Infrastructure Protection, and we are comprised of members that belong to both groups.
>
> "Under this dual structure, the priority of our infrastructure work requirements does come from the Office of Infrastructure Protection under the Assistant Secretary, Robert Stephan, but the approval of all the intelligence-derived production does remain with Mr. Charlie Allen, the new Assistant Secretary for Intelligence and Analysis.

[114] Statement of Melissa Smislova, Acting Director, Department of Homeland Security, Homeland Infrastructure Threat and Risk Analysis Center, before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, November 17, 2005, http://ftp.resource.org/gpo.gov/hearings/109h/35939.txt.

Figure 3. Section 201 Responsibilities of IAIP Under Secretary

Homeland Security Act of 2002, Section 201 Responsibilities of DHS Under Secretary for Information Analysis and Infrastructure Protection (partial listing*):*

(1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information in order to—

> (A) identify and assess the nature and scope of terrorist threats to the homeland;
>
> (B) detect and identify threats of terrorism against the United States; and
>
> (C) understand such threats in light of actual and potential vulnerabilities of the homeland.

(2) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

(3) To integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal government, State and local government agencies and authorities, the private sector, and other entities.

(4) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining such information from other agencies of the Federal government.

(5) To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems.

(6) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

> “The HITRAC mission represents a unique capability within the Federal Government. Our threat analysts have access to traditional Intelligence Community reporting and data, as well as to the DHS component intelligence and information reporting. Our HITRAC infrastructure protection sector specialists, on the other hand, who possess the private-sector expertise and sector-specific incident data, identify the sector-specific vulnerabilities and the consequences of a possible terrorist attack. Our HITRAC analysts then integrate all of this available information into strategic-level risk assessments for Federal, State and local authorities, as well as the private sector.
>
> “In addition, we believe that our intelligence products are more relevant to infrastructure owners and operators because we frame our analysis in the context and unique operating environment of our specific critical infrastructure partners.
>
> “We receive information about United States critical infrastructure through our Information Sharing and Analysis Centers, the ISACs, as well as through our contacts through the private and public infrastructure owners that have already been established by our colleagues in the Office of Infrastructure Protection and throughout the Preparedness Directorate. In addition, we are

able to refine our national-level Intelligence Community collection requirements by working back through the Office of Intelligence."

2.0 Mechanisms

This section reviews some of primary structures and mechanisms that are designed to enable critical infrastructure information sharing, including the sharing of intelligence information.

CIPAC

The Critical Infrastructure Partnership Advisory Council (CIPAC) directly supports the sector partnership model by providing a legal framework that enables members of the Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) to engage in joint CIKR protection-related discussions. CIPAC serves as a forum for government and private-sector partners to engage in a spectrum of activities, including:

- Planning, development, and implementation of infrastructure protection and preparedness programs.
- Operational activities related to infrastructure protection and resiliency, including incident response and recovery.
- Development and support of national policies and plans, including the National Infrastructure Protection Plan (NIPP) and Sector-Specific Plans (SSPs).

CIPAC membership consists of private-sector CIKR owners and operators, or their representative trade or equivalent associations from the respective sectors' SCC, and representatives of Federal, State, local, tribal, and territorial governmental entities (including their representative trade or equivalent associations) that make up the corresponding GCC for each sector.

Fusion Centers

The Department of Justice defines State and local fusion centers (fusion centers) as "a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[115] Fusion centers operate on the State and local level, with 72 currently operating in all 50 States and in 22 major urban areas.[116] These centers address the integrated information-sharing environment advocated by the 9/11 Commission by connecting Federal, State, local, tribal, and territorial intelligence.

A central tenet of fusion center baseline documents is that the mission of each fusion center should be developed locally and collaboratively to address the unique needs of its jurisdiction.[117] Recognizing that risks vary across the nation, fusion centers have tailored missions that distinguish the functions and

[115] U.S. Department of Justice and Department of Homeland Security, "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," Issued August 2006, pg. 2 http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf, accessed March 2011.

[116] U.S. Government Accountability Office, "Information Sharing: Federal Agencies are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results," September 2010, http://www.gao.gov/new.items/d10972.pdf

[117] U.S. Department of Justice, "Fusion Centers and Intelligence Sharing web page," http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181

outreach of each fusion center. While all centers were developed to improve intelligence-sharing, the missions, personnel, and funding vary based on the environment in which the fusion center operates.[118]

A number of fusion centers have chosen to incorporate their local private sector into a bi-directional information and intelligence-sharing partnership. These fusion centers have identified an important link between their missions and protecting and building more resilient critical infrastructure within their jurisdictions. This recognized value proposition drives varying degrees of fusion center engagement of critical infrastructure owners and operators. Nevertheless, differing operating environments can have different models—with some choosing to incorporate critical infrastructure and others choosing not to. Given their wide range of responsibilities and environments, the level of critical infrastructure involvement does not determine the overall efficacy of a single fusion center.

The mission of each fusion center is developed locally and collaboratively to address the unique needs of its jurisdiction.[119] The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) encourages fusion centers to implement critical infrastructure protection into their mission. This option has spurred a divergence of fusion center critical infrastructure-related capabilities. The four Critical Operational Capabilities (COCs) identified by the SLTTGCC for incorporating critical infrastructure into fusion center operations are defined as:

1. *Receive*—The fusion center has mechanisms in place to receive (process and collate) tips and leads from critical infrastructure entities relevant to the center's mission. The center has the ability to evaluate the information's validity and reliability and collate the collected information so relationships can be determined.
2. *Analyze*—The fusion center incorporates critical infrastructure-related analysis and develops products for critical infrastructure stakeholders to enhance protection of critical infrastructure.
3. *Disseminate*—The fusion center incorporates critical infrastructure stakeholders into their dissemination plan, including ensuring that appropriate information resulting from any of the fusion center's analytic products is provided to affected industry sectors and developing technology-assisted methods to distribute critical infrastructure information.
4. *Gather*—The fusion center incorporates critical infrastructure information requirements into their gathering and reporting strategy. The fusion center also reviews and, as necessary, updates their policies, processes, and mechanisms that are used for receiving, cataloging, and retaining information to ensure that critical infrastructure-related information is appropriately stored and protected.[120]

Table 1 conveys the divergence of private-sector outreach between the ideal practices that the private sector could harness and the actual practices today. Some fusion centers perform the ideal COCs and adapt their practices to reach their specific private-sector partners. Most fusion centers perform varying levels of COCs and the chart conveys the gap between where fusion centers are in actuality and their ideal COC goals. The "Ideal" characteristics are derived from the SLTTGCC Critical Infrastructure and Key Resources Protection Capabilities for Fusion Center and DHS Critical Operational Capabilities for State and Major Urban Area Fusion Centers as baseline resources. The "Actual" chart leverages the NIAC

[118] U.S. Government Accountability Office, "Information Sharing: Federal Agencies are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results,"

[119] U.S. Department of Justice, "Fusion Centers and Intelligence Sharing web page," http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181

[120] State, Local, Tribal, and Territorial Government Coordinating Council, *Critical Infrastructure and Key Resources (CIKR) Protection Capabilities for Fusion Centers.* December 2008. http://www.ncirc.gov/documents%5Cpublic%5Csupplementaries%5CCI_KR_Protection_Capabilities_Report.pdf

study's case study interviews and open-source research, as well as the Critical Operational Capabilities for State and Major Urban Area Fusion Centers, to create an accurate picture of the current status of fusion center private sector outreach capabilities.

Table 1: Fusion Center-Private Sector Interconnectivity

Critical Operational Capabilities (COCs)	Ideal/Optimal Role	Actual Role
Receive	• Fully-developed, tailored HSIN portals • Private sector access to secret and unclassified portals • Receipt of classified and unclassified information from the private sector • Appropriate handling and safeguarding of information or private sector information	• General e-mail/phone capabilities to receive inquiries/tips • Ad hoc reporting of threats from the private sector to its respective fusion center • Diverse set of State "Sunshine Laws" varying in degrees of protection for critical infrastructure information
Analyze	• Full-time critical infrastructure analyst(s) or a Critical Infrastructure Protection unit or desk with focus on critical infrastructure protection and resilience • Geographic, jurisdictional, and/or sector inventories • Site assistance visits/comprehensive reviews • Sector-specific assessment tools • Periodic data calls • Integrated critical infrastructure analysis with other agencies • Overlay international or national intelligence with State, local, and regional information to develop timely and actionable intelligence products for their respective critical infrastructure partners • Frame the intelligence in the context of their geographic area of responsibility • Sponsoring of critical infrastructure analytical training	• Law enforcement staff performing "all-hazard" analysis • Critical infrastructure threats and risks analyzed by fusion center; information not used to inform critical infrastructure protection threat landscape • "80% of fusion centers have procedures for information sharing and two-way communication with the private sector and CIKR owners and operators." • Forward open-source information that may or may not pertain to critical infrastructure partners • Procedures in place to share information with the private sector
Disseminate	• Fusion center analytic products provided to affected industry sectors • Feedback loop acknowledging receipt of critical infrastructure intelligence • Feedback loop also incorporate customer feedback (critical infrastructure owners and operators) regarding the quality, timeliness, and relevance of the fusion center's products into an informed production process	• Open-source threat information directed to sectors of importance for situational awareness • Fusion center receipt of critical infrastructure intelligence—no follow up after original information sharing—1 way information sharing • "The BCA results indicate that 63% of fusion centers do not have a feedback mechanism in place." (Continued)

Table 1: Fusion Center-Private Sector Interconnectivity (Continued)

Critical Operational Capabilities (COCs)	Ideal/Optimal Role	Actual Role

	• Routinely coordinating or modifying information requirements • Relevant analysis reported to appropriate Federal agencies • Technology-assisted methods to distribute critical infrastructure intelligence and information • Available and protected space for vetted critical infrastructure partners to share and receive sensitive information from their State and local fusion center	• No change to private sector information requirements despite lapse in time and evolving threat environment • Electronic alert blast to inform businesses about breaking news, alerts, possible threats, and suspicious activity
Gather	• Tracking and monitoring of Suspicious Activity Reports (SARs) from the private sector • Fully engaged in the implementation of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) • Site assistance visits • Utilization of associations • Information-sharing working groups designed to gather intelligence and sector intelligence needs (SINs) of private sector	• SAR mechanism for general public to report suspicious activity • General terrorism tip line • Privacy policy in place to protect shared information • Ad hoc calls with critical infrastructure partners

Critical Infrastructure and Key Resource Information Sharing Environment (CIKR ISE)

The DHS Office of Infrastructure Protection (IP) leads the coordinated effort to create a more protected and resilient critical infrastructure environment. Central to this complex mission is the effective and efficient sharing of information between public and private partners. IP facilitates the development and implementation of the Critical Infrastructure and Key Resource Information Sharing Environment (CIKR ISE) to enable informed decisions and timely actions among the 18 critical infrastructure sectors as they execute critical infrastructure protection and resilience activities.[121]

The mission of the CIKR ISE is guided by several national statutes, plans, and strategies. The Intelligence Reform and Terrorism Prevention Act of 2004 required the creation of an ISE to provide and facilitate the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The National Infrastructure Protection Plan (NIPP) directed IP to formulate an approach to information sharing that would support the 18 sectors. IP subsequently established the CIKR ISE in accordance with the National Strategy for Information Sharing and the ISE Implementation Plan. The Program Manager-ISE and the Federal inter-agency Information Sharing Council in 2007 adopted the CIKR ISE as an integrated part of the ISE and its primary private-sector component.

According to the PM-ISE, the resulting CIKR ISE provides a unifying, integrated framework for stakeholders from all levels of government and critical infrastructure owners and operators to communicate, coordinate and collaborate through the efficient exchange of timely and useful information pertinent to their shared mission of protection and resilience. It is a stakeholder requirements driven environment for process, technology, and content. The PM-ISE cited these recent CIKR ISE accomplishments in its 2011 annual report to Congress:

- *Homeland Security Information Network-Critical Sectors (HSIN-CS):* The number of active users on the CIKR ISE information-sharing platform, HSIN-CS, grew by 67 percent over the last year.

[121] DHS, "Information Sharing: A Vital Resource for a Shared National Mission to Protect Critical Infrastructure," web page, http://www.dhs.gov/files/programs/gc_1292350623062.shtm

Currently, a new user registers every 1.5 hours. New content is made available on HSIN-CS at a rate of every 2.5 hours. At the end of the 2nd quarter of FY 2011, 12,250 documents were available, representing a 100-percent increase over the same time last year.

- *Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)*: During the Deepwater Horizon Oil Spill, HITRAC produced and posted 31 products to HSIN-CS and Homeland Security Information Network-Emergency Management (HSIN-EM) to facilitate information sharing across the broad spectrum of response operations.
- *TRIPwire Community Gateway (TWCG)*: As part of the HSIN-CS, TWCG is designed to provide improvised explosive device (IED) awareness information specifically for the nation's critical infrastructure owners, operators, and private security personnel. TWCG provides expert threat analyses, reports, and relevant planning documents to help key private-sector partners anticipate, identify, and prevent IED incidents. Over the past year, the number of registered users increased by 63 percent.
- *HSIN Connect*: HSIN-Connect was utilized over the past year to host more than 28 educational events for approximately 17,500 critical infrastructure stakeholders. Briefing topics include critical infrastructure resilience, threat detection, protective actions, bête practices, and specific methodologies for CIKR tool training.[122]

Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

HITRAC is the Department of Homeland Security's critical infrastructure-intelligence center, incorporating analysts from the DHS Office of Infrastructure Protection and the Office of Intelligence and Analysis. HITRAC's mission is to create and disseminate threat and risk-informed analytical processes, services, and products that are practical, meaningful, timely, and directly beneficial to the development and prioritization of infrastructure protection strategies. HITRAC provides both steady-state and incident management capabilities to support DHS, Federal, State, local, and private sector decision making.

Since its inception, HITRAC has provided tailored risk-assessment products for critical infrastructure sectors, fusing consequence and vulnerability information (from infrastructure protection communities collected through IP) with threat information (from intelligence and law enforcement communities). Through access to a voluntarily identified network of sector experts from the Sector-Specific Agencies (SSAs) and Sector Coordinating Councils (SCCs), specialists and field-deployed Protective Security Advisors (PSAs), HITRAC products include: the CIKR National Risk Profile annually delivered to Congress; strategic risk assessments for each sector; threat handbooks; information bulletins; analytic reports on suspicious activity reports to sectors; and a supply-chain analysis.

HITRAC's steady-state activities identify and analyze threats, vulnerabilities, and consequences of attacks and other hazards for critical infrastructure risk-management and resilience planning. HITRAC's Risk Integration and Analysis Branch manages the National Critical Infrastructure Prioritization Program (NCIPP), a prioritized list of domestic critical infrastructure through the Level 1/Level 2 program, and internationally through the Critical Foreign Dependencies Initiative (CFDI). The Risk Development and Modeling Branch manages applied research to advance the state of homeland security risk analysis using transparent and flexible approaches and provides technical leadership for risk analysis and management efforts.

[122] Program Manager for the Information Sharing Environment, ISE Annual Support to Congress, June 2011, http://www.ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2011.pdf

During incidents of national significance, HITRAC is led by the Incident Planning and Response Branch. HITRAC's Incident Risk Analysis Cell (iRAC) serves as an integrating structure for HITRAC's analytic program. The iRAC taps into the center's steady-state programs and capabilities to provide immediate analytical support to decision makers in real time during the crisis. Assistance includes risk analysis, threat analysis, and consequence modeling conducted by the National Infrastructure Simulation and Analysis Center (NISAC). NISAC analysts provide real-time assistance to Department decision makers during such critical incidents as hurricanes, floods, wildfires, and manmade hazardous events.

Appendix K. Federal Programs and Processes

The following are Federal programs or partnerships utilized by critical infrastructure owners and operators relevant to the bi-directional sharing of intelligence information. Programs categorized as cross-cutting fuse multiple steps of the intelligence cycle. Other programs are categorized according to their primary focus on one particular piece of the intelligence cycle—Analysis, Collection, Dissemination, and Requirements.

Cross-Cutting Programs

Critical Infrastructure and Key Resources Information Sharing Environment (CIKR ISE) – The CIKR ISE, whose implementation is driven by stakeholder requirements, enables informed decisions and timely actions among the sectors as they execute infrastructure protection and resilience activities. Specifically, the CIKR ISE provides the procedures, content, and tools needed to enable security partners to share the vital information needed to manage their critical infrastructure security and risk, respond to events, and enhance resilience. The CIKR ISE's primary information sharing platform is the Homeland Security Information Network – Critical Sectors.

Critical Infrastructure Partnership Advisory Council (CIPAC)—DHS established CIPAC to facilitate effective coordination between Federal infrastructure protection programs with the infrastructure protection activities of the private sector and of State, local, territorial, and tribal governments. CIPAC membership consists of the critical infrastructure owner and operator members of all Sector Coordinating Councils (SCCs) and their corresponding Government Coordinating Councils (GCCs). CIPAC employs a special exemption, pursuant to section 871 of the Homeland Security Act to the Federal Advisory Committee Act, which protects from public disclosure certain SCC and GCC discussions containing sensitive critical infrastructure information. This exemption facilitates regular, ongoing, and multi-directional communications and coordination within CIPAC.

Domestic Security Alliance Council (DSAC)—DSAC is a strategic partnership between the FBI, the Department of Homeland Security and the private sector. DSAC enhances communications and promotes the timely and bidirectional exchange of information, keeping the nation's critical infrastructure safe, secure and resilient. DSAC advances elements of the FBI and DHS missions' in preventing, deterring, and investigating criminal and terrorism acts, particularly those effecting interstate commerce, while advancing the ability of the U.S. private sector to protect its employees, assets and proprietary information.

FBI InfraGard— InfraGard is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to mitigate threats to the nation's critical infrastructure. Eighty-six chapters affiliated with local FBI field offices cover all critical infrastructure sectors relevant to their region, with more than 40,000 members nationwide. Membership is free; businesses, academic institutions, and State and local law enforcement agencies are especially encouraged to join following a records check performed by the FBI.

Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)—HITRAC is the DHS infrastructure-intelligence fusion center, incorporating analysts from the Office of Infrastructure Protection and the Office of Intelligence and Analysis. HITRAC creates risk-informed analyses for Federal, State, local, tribal, territorial, private sector, and international partners.

Homeland Security Information Network—Critical Sectors (HSIN-CS)—HSIN is a national, secure, and trusted web-based portal for information sharing between partners engaged in the homeland security mission. Sector-specific portals enable the sharing of unclassified critical infrastructure information with and between CIKR owners and operators. Over 15,000 products are currently available on HSIN-CS, including incident reports, geospatial products, CIKR planning documents, and training and exercise opportunities.

"If You See Something, Say Something" Campaign—In July 2010, DHS launched a national "If You See Something, Say Something™" public-awareness campaign—a simple and effective program to raise public awareness of indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper State and local law enforcement authorities.

Interagency Threat Assessment and Coordination Group (ITACG)—The ITACG was enacted at the direction of the President and the "Implementing Recommendations of the 9/11 Commission Act of 2007" to enhance the sharing of intelligence with State, local, tribal, and private sector partners through established mechanisms within DHS and the FBI. The ITACG consists of Federal intelligence analysts and State, local, tribal, and territorial first responders working at the National Counterterrorism Center. The group evaluates and disseminates primarily overseas intelligence, providing a State/local/tribal/ territorial perspective to draft intelligence products.

National Information Sharing Environment (ISE)—The ISE was established by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 "for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties." IRTPA also established the Program Manager for the ISE, whose role is to "plan for and oversee the implementation of, and manage the ISE," and to be "responsible for information sharing across the Federal Government."

Nationwide Suspicious Activity Reporting Initiative (NSI)—The October 2007 National Strategy for Information Sharing called for the establishment of a "unified process for reporting, tracking, and accessing" Suspicious Activity Reports (SARs) in a manner that rigorously protects the privacy and civil liberties of Americans—what is now referred to as the NSI. It is an historic partnership among Federal, State, local, and tribal agencies as part of the national Information Sharing Environment. NSI establishes a national capacity for gathering, documenting, processing, analyzing, and sharing SARs, referred to as the SAR process.

Overseas Security Advisory Council (OSAC)—The OSAC acts as a liaison between the State Department security functions and the American private sector operating globally. This regular and timely sharing of information assists American companies in adapting to developments in the overseas security environment. Members of over 7,500 U.S. companies, educational institutions, faith-based institutions, and nongovernmental organizations are OSAC constituents.

Protected Critical Infrastructure Information (PCII) Program—The PCII Program is an information-protection program that enhances information sharing between the private sector and the government. DHS and other Federal, State and local analysts use PCII to analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures. If the information submitted satisfies the requirements of the Critical Infrastructure Information Act of 2002, it is protected from the Freedom of Information Act (FOIA), State and local disclosure laws, and use in civil litigation.

Protective Security Advisors (PSAs)—Trained critical infrastructure protection and vulnerability mitigation subject matter experts that advise and assist State, local, and critical infrastructure facility owners and operators on training, grants, and vulnerability assessments. The PSA program is viewed in the field as a success because it does not enforce regulations—a characteristic that fosters true partnerships—and has the ability to deliver Federal products and tools of significant value to State and local governments and critical infrastructure owners and operators.

Transportation Security Operations Center (TSOC)—Freedom Center—The TSOC has served as the coordination center for the Transportation Security Administration (TSA) during security incidents and operations since 2003. Every facet of TSA operations has a presence, and decisions are made and transmitted to the field in real time. The TSA Office of Intelligence can notify TSOC about developing situations. The Federal Air Marshal Service Mission Operations Center can be alerted and provide valuable feedback and guidance. TSOC also provides an avenue for reporting suspicious activity regarding pipelines.

United States Computer Emergency Readiness Team (US-CERT)— US-CERT is the operational arm of the National Cyber Security Division at DHS and is a public-private partnership that is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local government, industry, and international partners.

Analysis

Enhanced Critical Infrastructure Protection (ECIP) Assessment—The ECIP program and associated tools deployed in the field by Protective Security Advisors (PSAs) can substantially enhance State and local understanding of the characteristics of assets and systems.

Chemical Facility Anti-Terrorism Standards (CFATS)—Risk-based performance standards for the security of the nation's chemical facilities. Covered chemical facilities are required to prepare Security Vulnerability Assessments that identify facility security vulnerabilities, and to develop and implement Site Security Plans that include measures to satisfy identified risk-based performance standards.

National Infrastructure Simulation and Analysis Center (NISAC)—NISAC began as a collaborative effort between Los Alamos and Sandia National Laboratories in 1999 and was incorporated by the USA Patriot Act of 2001 into the DHS upon its inception in March 2003 and is overseen by DHS IP. The NISAC analyzes and monitors risk to the nation's critical infrastructure and provides key public and private-sector decision makers with risk-informed, analytic products that influence the prioritization of risk-reduction strategies. The NISAC conducts modeling, simulation, and analysis of the nation's critical infrastructure.

Collection

Automated Critical Asset Management System (ACAMS)—A non-regulatory, web-enabled information services portal that helps State and local governments build critical infrastructure protection programs in their local jurisdictions. ACAMS provides a set of tools and resources that help law enforcement, public safety, and emergency response personnel collect and use asset data, assess vulnerabilities, develop all-hazards incident response and recovery plans, and build public-private partnerships.

Dissemination

***Energy Assurance Daily (EAD)*—**The Department of Energy (DOE) produced Energy Assurance Daily provides a summary of public information concerning current energy issues. The EAD is published Monday through Friday to inform stakeholders of developments affecting energy systems, flows, and markets. It provides highlights of energy issues rather than comprehensive coverage.

Epidemic Information Exchange (Epi-X)—Epi-X is the Center for Disease Control's (CDC) web-based communications system for sharing information with public health officials. It provides rapid communications whenever there is a public-health need.

Roll Call Release—*Roll Call Release* is a collaborative, For Official Use Only (FOUO) product produced by the DHS Office of Intelligence and Analysis (I&A) and the FBI. The product is written specifically for State, local, and tribal (SLT) "street-level" first responders, focusing on terrorist tactics, techniques, procedures, terrorism trends, and indicators of suspicious activity. The success of this product can be measured by its incorporation into SLT-created publications and from the interest the product has drawn from international law enforcement partners.

Sector Classified and Unclassified Briefings—DHS provides sector-specific briefings to a number of sectors. Semi-annual classified briefings to Oil and Natural Gas (ONG) Sector Coordinating Council (SCC) members involve collaborative feedback on private-sector information needs. DHS IP also coordinates classified threat briefings for cleared members of the ONG Sector. To broaden the participation in these classified threat updates, DHS IP sponsors security clearances for members of the ONG SCC and employees of oil and natural gas companies and associations who have a need to be aware of such information. A variety of agencies, including DHS HITRAC, the Transportation Security Administration (TSA), the Federal Bureau of Investigation (FBI), DOE, and other members of the intelligence community, provide briefings at these semi-annual events.

Requirements

Sector Intelligence Needs (SINs)—Through numerous Federal authorities, DHS is charged with identifying intelligence requirements in conjunction with critical infrastructure partners. In recent years, the ONG Sector has worked closely with DHS I&A to develop Sector intelligence needs (SINs) through a dialogue with DHS to discuss threat concerns and intelligence needs from the perspective of the ONG Sector. Both the Sector and DHS identified the need to collect specific input from Sector members, to improve government analysts' intelligence-gathering capabilities, and to generate more useful intelligence products and classified briefings.

Appendix L. Homeland Security Information Network – Critical Sectors

Homeland Security Information Network

The *Homeland Security Act of 2002* assigned DHS the responsibility to coordinate the Federal Government's homeland-security communications with State and local government, the private sector, and the public. The Act required DHS to establish the necessary information technology for sharing homeland security information without duplicating existing networks or systems. The Joint Regional Information Exchange System (JRIES) was widely used in multiple communities and regions; and to avoid duplication of systems and networks, it was selected by DHS to form the backbone of the Homeland Security Information Network (HSIN). A brief history of HSIN and implications for the critical sectors component of HSIN (HSIN-CS) is shown in Table 1.

Table 1. HSIN Timeline

Year	Activity	Implications for HSIN-CS
2002	Homeland Security Act passed by Congress and signed into law.	Requires DHS to establish necessary information technology for sharing homeland security information.
2004	HSIN is implemented with JRIES serving as the foundation. JRIES is based on a law-enforcement mission.	JRIES requirements do not directly address the requirements of the critical infrastructure sectors.
2005	The Office of Management and Budget released Circular A-11	A-11 directs agencies to reduce project risk by involving stakeholders in the design of IT assets
2006	HSIN is designated as the official system for operational sensitive but unclassified (SBU) information sharing within DHS and with its partners.	HSIN – CS is established. HSDN serves as the companion portal for sharing Secret-level intelligence.
2006	DHS Office of the Inspector General identifies challenges with HSIN implementation. DHS OIG found that "DHS developed HSIN using the same requirements obtained for JRIES…"[123]	DHS OIG states DHS did not sufficiently involve non-law-enforcement users in the initial design of HSIN; the requirements "did not address the additional communities that HSIN had included . . ."
2007	HSIN Advisory Committee established within the provisions of the Federal Advisory Committee Act (FACA). [124] The Committee is composed of 20 members from different homeland security areas.	Provides independent advice and recommendations to DHS leadership on HSIN; charter reserves 3 seats for private sector for a "balance of perspective."
2009	New National Infrastructure Protection Plan is released.	Within HSIN-CS, each sector establishes the rules for participation
2010	HSIN transitions from the Operations Coordination and Planning Directorate to the Office of the Chief Information Officer (OCIO).	HSIN is now managed by the organization with information management as its core capability
2011	The *Final Business Case* for HSIN is approved. U.S. Secret Service (USSS) partners to become a content provider on HSIN-CS.	Outlines a new path for meeting the needs of different mission communities. Integrates USSS information within HSIN-CS to enhance information sharing with the Banking and Finance Sector and others.
2012-2013	Full deployment of HSIN release 3.	Staged deployment of newest release, based on new platform and user-specific requirements, with comprehensive training plan for all HSIN users and communities.

[123] U.S. Department of Homeland Security, Office of Inspector General. "Information Sharing with Fusion Centers has Improved, but Information System Challenges Remain," October 2010, http://www.oig.dhs.gov/assets/Mgmt/OIG_11-04_Oct10.pdf

[124] U.S. Department of Homeland Security. "Homeland Security Information Network Advisory Committee Charter," (RENEWED), http://www.dhs.gov/xlibrary/assets/hsinac_charter.pdf

HSIN is the primary platform utilized by DHS for sharing sensitive unclassified information. The Homeland Security Data Network (HSDN) serves as a companion portal and provides SECRET-level connectivity to State and local fusion centers to receive Federally generated classified threat information.

HSIN forms the foundation of a number of communities of interest that serves a range of security stakeholders, including:

- Critical Sectors
- Defense
- Emergency Management
- Homeland Security
- Intelligence
- International
- Law Enforcement
- Multi-Mission

These communities have attempted to adapt the HSIN structure to user requirements. In addition to supporting the original user community of law enforcement and intelligence professionals, HSIN has progressively added user communities in areas such as emergency management and critical infrastructure. Due to the far-reaching functions and requirements needed by these communities, HSIN usage is divergent among the various communities, sectors, and levels of government in which it is deployed. HSIN is intended to be a user- and sector-driven environment. This, however, infers active and engaged participation to tailor the portal to its appropriate end-users.

A 2006 DHS Office of Inspector General Report found that DHS did not sufficiently involve users in the initial design of HSIN. As JRIES and then HSIN were used as a system of convenience to avoid duplication, "DHS developed HSIN using the same requirements obtained for JRIES…" These requirements did not address the additional communities that HSIN had included, and instead were based off of a functional working group of 25 law enforcement officials.[125] DHS subsequently created individual community portals, with the expectation that each community would tailor their portal to their requirements.

Homeland Security Information Network – Critical Sectors

As part of National Infrastructure Protection Plan's strategic approach information sharing, the National Protection and Programs Directorate, Office of Infrastructure Protection created the Critical Infrastructure and Key Resources Information Sharing Environment (CIKR ISE). The CIKR ISE is primarily hosted on HSIN-CS, which is dedicated solely to supporting critical infrastructure and resilience activities. HSIN-CS is intended to facilitate a bi-directional information flow between DHS, owners and operators, and other mission partners.

Access to HSIN-CS is intended for vetted critical owners and operators and their government partners. Although sector- and user-driven, HSIN-CS varies in its usage across the sectors. A November 2011 Government Accountability Office (GAO) report on transportation information sharing found that almost 60 percent of those surveyed had never heard of HSIN-CS.[126] The GAO report went on to explain that without the input of industry committees, DHS cannot develop HSIN-CS to meet the needs of aviation stakeholders.

[125] U.S. Department of Homeland Security, Office of Inspector General, "Homeland Security Information Network Could Support Information Sharing More Effectively," June 2006. http://www.oig.dhs.gov/assets/Mgmt/OIG_06-38_Jun06.pdf

[126] U.S. Government Accountability Office, "Transportation Security Information Sharing: Stakeholders Generally Satisfied but TSA Could Improve Analysis, Awareness, and Accountability." November 2011. http://www.gao.gov/new.items/d1244.pdf

As a user-driven portal, HSIN varies according to the level of user participation and buy-in. NIAC interviews demonstrated this variance in HSIN usage: some interviewees preferred other information-sharing mechanisms they found more useful than HSIN-CS, and some indicated that HSIN-CS was one of many helpful mechanisms. Current user statistics for HSIN-CS show a wide variation in both the number of users and how often the users access HSIN-CS. This participant variation, on a sector- and user-driven portal, conveys the wide-ranging HSIN-CS value proposition across the private sector.

While acknowledged as a helpful reference tool for familiar users, users generally cited HSIN-CS as difficult to use and not providing information in real-time. NIAC interviews revealed that HSIN-CS often does not provide significant value to the private sector compared to other approaches—e.g., use of Information Sharing and Analysis Centers, or private security firms. An examination of the individual comments across all the case studies reveals the following observations:

General

Since its inception, HSIN-CS has gradually improved, but does not yet meet the needs of many sectors.

- Sectors that use HSIN-CS most extensively seem to view it as a cost-effective tool. The SCCs may make this determination after a comparison with alternative information sharing approaches.
- Some of the SSAs use HSIN-CS effectively, some do not – sometimes because they have their own information sharing networks with their private sector stakeholders.
- Users have divergent expectations about the content, timing, and functionality of HSIN-CS.

Content

The network is generally thought to be a useful resource for background information, but the use of this type of information varies greatly from the perspective of those interviewed. Some consider the information to be overly broad and too sanitized, and not provided in sufficient context or with analytic insight, to be useful.

- HSIN-CS is considered by some users to be an excellent source for training tools.
- The network is considered to be a good place to learn general threat information, so some of those interviewed stated they try to promote the system to as many people as possible within their sector.
- The usefulness of content is determined by user-driven requirements, which require active engagement by the sectors.
- There is uncertainty as to the distribution restrictions on U/FOUO information posted on the sites.

Timing

- The fact that HSIN-CS does not provide real-time information limits its usefulness during fast-moving crises. After-the-fact analysis is generally not the most important information to users.
- The teleconferencing capabilities of HSIN-CS are very useful during events such as hurricanes.

User Community

HSIN-CS can be improved and modified to meet the needs of individual portal users. It is not intended to be a top-down driven network but rather a user-defined/modified network. However, few of those interviewed seemed to recognize that this is the model, nor do they have the time to work with DHS to improve the network or the content.

- HSIN-CS is a pull system, in that most users have to directly access the information they seek. Many comments across the case studies indicated that "pushing" critical or time-sensitive information out to the users would be very useful.
- HSIN-CS has very limited exposure among end users in most of the sectors. It clearly is an under-utilized information tool. Within a single company, often only a few of the potential users have access or knowledge of the system.
- If HSIN-CS is not used, people will forget about it. Ongoing outreach and education are needed to promote buy-in and use by potential users.

Operations/Administrative

- The interface is difficult to navigate, resulting in considerable time being spent to locate the needed information.
- Many of those who have access to HSIN-CS do not like the frequent change of passwords, the difficult-to-learn organization of the interface, and the time it takes of locate information or documents. It is not thought to be user-friendly.
- All users have to be vetted before given access to HSIN-CS. While this is a requirement for systems with For Official Use Only (FOUO) information, it can be time consuming and frustrating to some.
- HSIN-CS is one of many systems used, all requiring different passwords. A single login would be welcomed, because no single system contains all the information the user needs.

HSIN-CS Effective Practices

Despite its disparate usage, HSIN-CS has been adapted to the needs of some of its end users and has been deployed to support information sharing environments in various capacities. The two following examples demonstrate the adaptive capabilities of HSIN-CS in the Dams Sector and the Northern California Regional Intelligence Center (NCRIC). It is important to note that a common success factor is the proactive engagement by the user community to define their specific information requirements and delivery preferences, including the use of an information sharing working group dedicated to the effort.

Dams Sector

The Dams Sector is actively engaged in promoting and leveraging HSIN-CS capabilities for its sector use. The HSIN-CS Dams Portal offers a Suspicious Activity Reporting tool that gives sector partners the opportunity to better understand the implications of incidents that occur throughout the Nation by examining reports from a broad range of sector stakeholders and subsequently determining any need to implement protective measures. The sector also conducts public/privates collaboration to produce and disseminate sector-specific critical infrastructure protection products. The Security and Education Working Group is composed of public and private Dams Sector members whose primary role is to introduce relevant critical infrastructure protection information and distribute this information throughout the Dams sector. Specifically, the working group posts this information on the HSIN-CS Dams portal and other interest-specific portals relevant to Dams owners and operators.

Northern California Regional Intelligence Center
Currently, eight fusion centers are actively engaged in the CIKR ISE and currently use or plan to use HSIN-CS to share information with private sector stakeholders. The NCRIC was the original fusion center pilot for the roll-out of the CIKR ISE. Joining the CIKR ISE in June 2009, the fusion center immediately began to leverage the support of the Office of Infrastructure Protection to amplify its outreach to the region's private sector. The NCRIC's Private Sector Advisory Council, drawn from entities across multiple sectors in Northern California, serves as the Information Sharing Working Group (ISWG). Using collaborative discussions, Webinars, and a half-day in-person workshop, the ISWG coordinated with NPPD/IP to design a highly functional ISE that meets their communication and coordination requirements. This tailored space is comprised of sub-portals created specifically for local critical infrastructure partners.

This value was conveyed during the trial of a former Bay Area Rapid Transit police officer in 2010. The Regional Incident Discussion Board on HSIN-NCRIC provided a vital link between infrastructure owners and operators, the fusion center, and the respective emergency operations centers activated in advance of the trial verdict. As riots erupted in downtown Oakland, the rapid communications enabled through HSIN-NCRIC led to the safe closure and restoration of businesses in the downtown Oakland area.

Path Forward

HSIN-CS continues to mature to address the information-sharing requirements of its critical infrastructure stakeholders. Several major changes over the past year will influence the portal's gradual evolution. Coupled with its varied success in the field, these changes should position HSIN-CS to better meet the requirements of critical infrastructure stakeholders. Several key characteristics will guide the overall HSIN path forward.

Clear Mandate and Mission
DHS released its *Final Business Case for Homeland Security Information Network* in 2011, which considered alternatives to legacy HSIN. The DHS Office of Chief Information Officer (OCIO) analyzed each alternative on its ability to meet key user and program requirements. The business case recommended that DHS should focus on updating the legacy HSIN to a current version of its existing technology. This decision has been overwhelmingly supported the leadership across DHS and is reflected throughout the Department. As one example of this development, in 2011 the U.S. Secret Service became a formal content provider on HSIN-CS.

Strengthened Management and Oversight
Management of HSIN has transitioned from the Operations Coordination and Planning Directorate to the DHS Office of the Chief Information Officer (OCIO). The OCIO identified performance metrics for HSIN to continue its growth and has provided the strategic and tactical management oversight necessary to mature HSIN. While DHS acknowledges major HSIN issues, the OCIO is better positioned to address and remedy program risks. A comprehensive Performance Management Plan, to be completed in 2011-2012, will allow the HSIN Program Office to measure HSIN's progress against stated program objectives such as effectiveness, efficiency, and customer satisfaction in a number of key areas.

Building on Lessons Learned
While HSIN's acceptance has varied widely across sectors, the systems' evolution will build on lessons learned - from success stories as well as from failures. HSIN-CS currently has 10,000 vetted critical infrastructure owners and operators and partners from over 1,500 government and private sector organizations. A new owner and operator joins HSIN-CS every 1.5 hours. DHS organizations and other Federal agencies are also utilizing HSIN during incidents. For example, during the Deepwater Horizon

response, the U.S. Coast Guard chose HSIN as the only platform that could provide interagency information sharing and coordination. As a result of this experience, the U.S. Coast Guard updated its incident response plan to designate HSIN as the portal of choice for information sharing.

Conclusion

The HSIN platform has struggled to evolve from the original JRIES system. Non-law-enforcement information needs were increasingly required as the homeland security mission community continued to expand. As the communities of interest proliferated, however, DHS was slow to raise sufficient awareness among stakeholders about tailoring the portals to their explicit needs. To ensure HSIN's success as a user-driven tool, DHS needs to assure that there is adequate outreach and education to facilitate active sector engagement and participation in HSIN-CS.

Although DHS and its stakeholders have witnessed numerous HSIN developmental delays, its current status, with strengthened management and identification of a clear mandate and mission, appear to set HSIN on a promising path forward. The constructive steps undertaken by DHS OCIO demonstrate a renewed level of senior-level oversight and management. Nonetheless, based on interviews from this report's case studies, the acceptance and use of HSIN-CS as a *commonly used tool* for information sharing is not certain. Sustained DHS senior-level oversight will be essential to realizing the goals of the *Final Business Case*.

Appendix M. Fusion Centers and their Role in Intelligence Sharing with the Private Sector

1.0 Introduction

The Department of Justice defines State and local fusion centers as "a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[127] Fusion centers operate on the State and local level, with 72 currently operating in all 50 States and in 22 major urban areas.[128] These centers address the integrated information-sharing environment advocated by the 9/11 Commission by connecting Federal, State, local, tribal, and territorial intelligence.

A central tenet of fusion center baseline documents is that the mission of each fusion center should be developed locally and collaboratively to address the unique needs of its jurisdiction.[129] Recognizing that risks vary across the nation, fusion centers have tailored missions that distinguish the functions and outreach of each fusion center. While all centers were developed to improve intelligence-sharing, the missions, personnel, and funding vary based on the environment in which the fusion center operates.[130]

A number of fusion centers have chosen to incorporate their local private sector into a bi-directional information and intelligence-sharing partnership. These fusion centers have identified an important link between their missions and protecting and building more resilient critical infrastructure and key resources (CIKR) within their jurisdictions. This recognized value proposition drives varying degrees of fusion center engagement of critical infrastructure owners and operators. Nevertheless, differing operating environments can have different models—with some choosing to incorporate critical infrastructure and others choosing not to. Given their wide range of responsibilities and environments, the level of critical infrastructure involvement does not determine the overall efficacy of a single fusion center.

2.0 Types of Information-Sharing Activities

There are four general categories of fusion-center activity related to critical infrastructure.

Operating a Specialized Critical Infrastructure Protection (CIP) Unit

A number of State and local fusion centers have integrated a critical infrastructure-focused unit into their operations to implement activities such as conducting threat assessments, communicating directly with critical infrastructure owners and operators, and analyzing trends and threats. The Massachusetts Commonwealth Fusion Center's specialized CIP unit offers strategic assessments and a collaborative information-sharing environment with the private sector. The Michigan Intelligence Operation Center CIP Desk is customized to collaborate with, provide intelligence to, and receive intelligence from the

[127] U.S. Department of Justice and Department of Homeland Security, "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," Issued August 2006, pg. 2 http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf, accessed March 2011.

[128] U.S. Government Accountability Office, "Information Sharing: Federal Agencies are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results," September 2010, http://www.gao.gov/new.items/d10972.pdf

[129] U.S. Department of Justice, "Fusion Centers and Intelligence Sharing web page," http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181

[130] U.S. Government Accountability Office, "Information Sharing: Federal Agencies are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results."

State's critical infrastructure owners and operators. The Florida Counter Terrorism Intelligence Center, for example, performs strategic assessments on critical infrastructure throughout the State.[131]

Disseminating Sector-Specific Threat Reports

Other State and local fusion centers analyze threats and disseminate information regarding impacts to *specific critical infrastructure sectors* within their jurisdiction. These centers examine State and local suspicious activity as well as national and international incidents that may have a nexus with their jurisdiction's sectors. The Colorado Information and Analysis Center provides a current threat overview of critical infrastructure sectors being targeted nationally and internationally, such as for the Chemical Sector. The Arizona Counter Terrorism Intelligence Center disseminates open-source threat information that could apply to its private-sector partners, such as a report forwarded for situational awareness on hacking of hotel networks. The Michigan Intelligence Operation Center provides specific monthly threat reports to CIKR owners and operators that detail suspicious activity concerning critical infrastructure in Michigan during the previous month, analysis of suspicious activity, and a follow-up on suspicious activity outcomes (i.e., arrests, questioning, further investigation, etc). This in-depth monthly reporting is also used to identify spatial, monthly, and suspicious event trends.[132]

Distributing Regular, Open-Source Suspicious Activity and Threat Reports

Some State and local fusion centers also distribute to their private-sector partners regular (i.e., weekly or monthly) open-source suspicious-activity and threat reports *pertaining generally* to the jurisdiction's critical infrastructure. These open-source compilations are intended to provide private-sector partners situational awareness of threats without focusing on a specific sector. The North Dakota State and Local Intelligence Center compiles a weekly unclassified, open-source product that documents threats and accidents pertaining to North Dakota as well as national and international critical infrastructure. The Georgia Information Sharing and Analysis Center releases a weekly summary of open-source information concerning terrorism and infrastructure issues of interest to Georgia's homeland security community and critical infrastructure sectors.[133]

Gathering Suspicious Activity Reports from the Sectors

Certain State and local fusion centers have incorporated the National Suspicious Activity Reporting Initiative into their operations to gather and manage the bi-directional flow of Suspicious Activity

[131] Commonwealth Fusion Center, Massachusetts, "Commonwealth Fusion Center flier," http://www.mass.gov/Eeops/docs/msp/homeland_security/terrorism/fusion_center/fusion-center-brochure.pdf,.: Michigan Intelligence Operations Center (MIOC), "Critical Infrastructure Protection (CIP) Desk webpage," 2001-2011, http://www.michigan.gov/mioc/0,1607,7-241-44728-168024--,00.html,.: Florida Department of Law Enforcement, "Investigations & Forensic Science Program Office: Office of Statewide Intelligence web page," http://www.fdle.state.fl.us/content/getdoc/595aab23-67a2-4dd8-9bdb-e0dac2f25559/OSI-Home.aspx

[132] Colorado Information and Analysis Center, "Infrastructure Sector Threat Report: CHEMICAL SECTOR," http://www.denvergov.com/Portals/428/documents/CIAC-Threat%20Report%20Chemical%20Sector.pdf; Arizona Counter Terrorism Intelligence Center (ACTIC),
Partners for Arizona's Safety & Security (P.A.S.S), "Hospitality Industry Hit Hardest by Hacks," February 8 2010, http://www.azactic.gov/Bulletins/Documents/AZP10001.pdf,. Michigan Intelligence Operations Center (MIOC), "Monthly CIKR Monitor," Released Monthly, Scott Raeder (Energetics) received August CIKR Monitor 2010 from Jim Harkness, Michigan State Police and CIP Desk.

[133] North Dakota State and Local Intelligence Center (NDSLIC), "The North Dakota Homeland Security Anti-Terrorism Summary," February 22 2011, http://www.nd.gov/des/uploads/resources/569/nd-all-source-anti-terrorism-02-22-2011.pdf.: Georgia Information Sharing and Analysis Center (GISAC), "Open Source Report," Released weekly,
http://www.gema.ga.gov/rss_generator.nsf/rss?openagent&uid=ECEED8851649594885257564006DE25

Reports (SARs) to and from the private sector. The Dallas Police Department's Fusion Center manages a SAR program, called iWatch Dallas, with its private-sector participants. Submitted SAR information is gathered and reviewed by a Private Sector Coordinator, who also acts as a direct point-of-contact and support for critical infrastructure needs and activities. The Southern Nevada Counter Terrorism Center, the Virginia Fusion Center, and the New York State Intelligence Center have also implemented similar programs for managing SARs with their respective private-sector partners.[134]

3.0 Examples of Fusion Centers with a Critical Infrastructure Function

Eight fusion centers have been identified as regularly performing key activities related to performing the critical infrastructure protection function. They are:

- Arizona Counter Terrorism Intelligence Center (ACTIC)
- Boston Regional Intelligence Center (BRIC)
- Dallas Fusion Center
- Michigan Intelligence Operations Center (MIOC)
- Northern California Regional Intelligence Center (NCRIC)
- New York Police Department Real Time Crime Center: Counter Terrorism - Lower Manhattan
- Southern Nevada Counter Terrorism Center (SNCTC)
- West Virginia Intelligence Fusion Center

The following includes a brief description of these eight centers and their private-sector information-sharing activities.

Arizona Counter Terrorism Intelligence Center (ACTIC)

The Arizona Counter Terrorism Intelligence Center opened in 2004 as the Nation's first fusion center. The ACTIC has chosen to actively incorporate the efforts of State, county, and local agencies that are already involved in working with the private sector in securing their facilities and accomplishing all-hazards preparedness.[135] Through formal liaisons, the ACTIC develops relationships with private-sector partners to develop a bi-directional communication mechanism. The following are key components of the ACTIC's interaction with Arizona's private sector:

- *Partners for Arizona's Safety & Security (PASS)* — ACTIC is actively engaged in the public-private partnership AZ PASS as the central medium for receiving, disseminating, and gathering intelligence from the State's 19 critical infrastructure sectors (hospitality is included as the 19th sector due to its importance to Arizona). AZ PASS is a partnership of the ACTIC, the Arizona Division of Emergency Management (ADEM), DHS, Phoenix InfraGard, and private-sector

[134] Dallas Police Department, "iWatch Dallas.net website," http://www.dallaspolice.net/index.cfm?page_ID=10170&subnav=53&openid=11.: Southern Nevada Counter Terrorism Center (SNCTC), "SAR Form," http://www.snctc.org/index.asp,.: Captain Doug Keyer, New York State Police, and Director, New York State Intelligence Center; and Lehew W. Miller III, Lieutenant, Virginia State Police, and Director, Virginia Fusion Center, "Nationwide SAR Initiative Delivers Value to Fusion Centers," *The Police Chief Magazine*, February 2011, http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=2311&issue_id=22011

[135] Federal Emergency Management Agency (FEMA), "State Partnership—Arizona," March 2011, http://www.fema.gov/pdf/privatesector/arizona_ppp.pdf

companies throughout Arizona. AZ PASS members can make critical infrastructure-related queries directly to the ACTIC.[136]

- *Community Liaison Program (CLP)* –The CLP acts "as a conduit for assimilating information to and from law enforcement agencies into impacted communities," including the private sector.[137] This liaison facilitates the ability to receive and gather information through a redaction process that synthesizes information and intelligence from multiple sources (DHS/FBI, law enforcement, terrorism liaison officers) into one single form. The program has grown to include 4,000 representatives representing 300 private and public-sector organizations across Arizona.
- *Analysis and Dissemination*—The ACTIC and ADEM disseminate regular "One Page Notes", an executive summary of current events in the private sector. The ACTIC also disseminates open-source threat information to AZ PASS members that could apply to its private-sector partners, such as a report forwarded for situational awareness on hacking of hotel networks.[138]

Boston Regional Intelligence Center (BRIC)

The Boston Regional Intelligence Center gathers intelligence to make more informed judgments and take the necessary action to counter the activities of criminals and terrorists.[139] The BRIC disseminates regular (i.e., weekly or monthly) open-source suspicious-activity and threat reports to the region's private-sector partners. (For example, the BRIC released a situational-awareness report on suspicious white powder in letters being sent to area hospitals.) These unclassified compilations are intended to provide private-sector partners situational awareness of threats or potential threats.

Dallas Fusion Center

The Dallas Fusion Center was created in 2007 as the Nation's 40th fusion center. The center acquired full staffing and expanded to full-time operations in 2008.[140] The center engages its local owners and operators through two central efforts to gather suspicious-activity intelligence from the private sector. They are:

- *iWatch Dallas* – The Dallas Fusion Center has developed its own effort, iWatch Dallas, to incorporate suspicious activity into fusion centers by gathering and managing the bi-directional flow of Suspicious Activity Reports (SARs) to and from the private sector. Suspicious activity can be reported via e-mail, text, online, or by phone.[141]
- *Private Sector Coordinator* – Submitted SAR information is gathered and reviewed by a Private Sector Coordinator that supports local critical infrastructure needs and activities. The coordinator is a specialized Detective that provides a direct point-of-contact for the private

[136] Ibid.

[137] Arizona Counter Terrorism Information Center, "Community Liaison Program, website," http://www.azactic.gov/Community_Liaison/

[138] Arizona Counter Terrorism Information Center, "Hospitality Industry Hit Hardest By Hacks," February 8, 2010. http://www.azactic.gov/Bulletins/Documents/AZP10001.pdf

[139] Boston Police Department, "Boston Police Department Virtual Community," http://www.bpdnews.com/about/programs/

[140] "Dallas Police Department Fusion Center Update," Metro Operations Support and Analytical Intelligence Center (MOSAIC), Public Safety Committee, June 15, 2009. http://www.dallascityhall.com/committee_briefings/briefings0609/PS_Fusion_Center_061509.pdf

[141] Dallas Police Department, "IWatchDallas. Do You?" flyer, http://www.dallaspolice.net/content/11/66/uploads/dpd091510dp02_smaller.pdf

sector and establishes a familiar relationship and medium for the region's private sector to share intelligence.[142]

Michigan Intelligence Operations Center (MIOC)

The Michigan Intelligence Operation Center's Mission Statement is "To promote public safety by operating in a public-private partnership that collects, evaluates, analyzes, and disseminates information and intelligence in a timely and secure manner while protecting the privacy rights of the public."[143] The MIOC actively engages Michigan's critical infrastructure owners and operators. The MIOC Critical Infrastructure Protection (CIP) Desk is customized to collaborate with, provide intelligence to, and receive intelligence from the State's critical infrastructure owners and operators. The MIOC also provides specific monthly threat reports to critical infrastructure owners and operators that detail suspicious activity concerning critical infrastructure in Michigan during the previous month, analysis of suspicious activity, and a follow-up on suspicious activity outcomes (i.e., arrests, questioning, further investigation, etc). This in-depth monthly reporting and analysis is also used to identify spatial, monthly, and suspicious event trends.

Northern California Regional Intelligence Center (NCRIC)

The mission of the Northern California Regional Intelligence Center is to "coordinate the exchange of criminal intelligence, threats, and hazards and facilitate regional communication among Northern California Law Enforcement, First Responders, Government, and Private Sector Partners."[144] The NCRIC helps its private-sector critical infrastructure owner and operator members prepare for incidents through heightened vigilance. Outreach to the private sector includes receiving, gathering, and analyzing trends to assess threats to the region's critical infrastructure. The NCRIC employs a full-time Private Sector Liaison Officer who provides a direct point of contact at the fusion center for the region's CIKR owners and operators. The private sector is formally organized around its Private Sector Information Sharing Workgroup and Infrastructure Protection Advisory Council. The private sector participates in a weekly suspicious-activity conference call hosted by the NCRIC.[145]

The Private Sector Information Sharing Workgroup is directly involved in outreach decisions, such as the development of the Homeland Security Information Network (HSIN-CS) NCRIC portal. This direct engagement of the private sector ensures the information-sharing needs of the private sector are strongly considered. This tailored space in HSIN-NCRIC provides access to local subportals and grants direct access for critical infrastructure owners and operators to the NCRIC, where they can submit tips, questions, or suggestions. This function facilitates the process of receiving information from the private sector by the NCRIC and helps the NCRIC to disseminate advisories, bulletins, and alerts to the private sector.

NYPD Real Time Crime Center: Counter Terrorism - Lower Manhattan (RTCC)

The New York Police Department launched the Real Time Crime Center in 2005 with the goal of creating a centralized technology center to support field officers and detectives on a full-time basis with comprehensive data to identify trends and fight crime. The center supports more than 53,000 uniformed and civilian members of the department who require more than 4,000,000 transactions and

[142] Dallas Police Department, "SAR Form."

[143] Michigan Intelligence Operations Center, "Michigan Intelligence Operations Center for Homeland Security, web page," http://www.michigan.gov/mioc

[144] Northern California Regional Intelligence Center, "Northern California Regional Intelligence Center, webpage," https://ncric.org/default.aspx?AspxAutoDetectCookieSupport=1

[145] Brandon Bond, "Private Sector Partnership," presentation, December 10, 2009.

thousands of queries annually for investigative work.[146] The RTCC works in conjunction with the Lower Manhattan Security Initiative, a program that links public and private-sector surveillance cameras (as well as license-plate scanners and chemical and biological sensors) to the center.[147]

Southern Nevada Counter Terrorism Center (SNCTC)

The Southern Nevada Counter Terrorism Center regularly participates in private-sector outreach to the region's critical infrastructure owners and operators. Following the attacks on hotels in Mumbai, the SNCTC collaborated with Las Vegas hotels and casinos to train their respective staffs on suspicious behaviors associated with terrorism. The SNCTC has also developed a "Critical Infrastructure Protection System," an electronic tool that provides first responders throughout Nevada with vital critical infrastructure information, such as floor plans, locations of hazardous materials, and updated 360-degree video of important local facilities.[148] The SNCTC also developed the Private Sector SAR Sharing Initiative (PS3), a web-based application that allows facilities to capture and record suspicious activities, including video or photos. The PS3 has linked into the National Suspicious Activity Reporting (SAR) Initiative (NSI). When a suspicious activity is vetted by SNCTC analysts and found to meet the criteria for the NSI, the report is uploaded into "shared space" where other fusion centers can access the report. [149]

West Virginia Intelligence Fusion Center

The West Virginia Intelligence Fusion Center was opened in March 2008 "to detect, prevent, vet, and respond to information concerning criminal and terrorist activities and all other crimes and hazards…"[150] The West Virginia Intelligence Fusion Center works in conjunction with the State Protective Security Advisor (PSA), the National Guard, and other State and local agencies to perform valuable outreach and foster a bi-directional information-sharing partnership with the State's private sector. The fusion center releases an all-sectors weekly report to the private sector that documents all-source threats. For individual incidents, the center releases a more targeted report.

4.0 Present State of Fusion Center Critical Infrastructure Involvement

Private-sector representatives have a history of collaborating on the establishment and focus of fusion centers. Critical infrastructure owners and operators participated in the development of the *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era (Guidelines)*. The *Guidelines* recognized that "data fusion involves the exchange of information from different sources—including law enforcement, public safety, and the private sector," that can result, with analysis, in "meaningful and actionable intelligence and information." Subsequent guidance from The *Critical Infrastructure and Key Resources Protection Capabilities for Fusion Centers*, released in December 2008, *encourages, but does not require,* fusion centers to implement critical infrastructure protection into their mission. This option has resulted in a disparity of private-sector outreach activities and capabilities.

[146] Tim Burke and Dees Stribling, "Top agencies utilize state-of-the-art technology," *Public Safety IT Magazine*, November 2010, http://www.hendonpub.com/resources/articlearchive/details.aspx?ID=208133,.

[147] Michael Coe, "To investigate the practice and implementation of Designing out Crime and the use and effectiveness of Closed Circuit Television (CCTV) in public places." The Winston Memorial Trust of Australia, 2008, http://www.churchilltrust.com.au/site_media/fellows/Coe_Michael_2008.pdf.

[148] Lt. Tom Monahan, Director, Southern Nevada Counter-Terrorism Intelligence Center, "Safeguarding America's Playground," Guest Column, University of Nevada Las Vegas Institute for Security Studies, July/August 2010, http://iss.unlv.edu/Guest%20Columns/guestcolumn-julyaugust%202010.html,.

[149] Ibid.

[150] West Virginia Intelligence Fusion Center, "West Virginia Intelligence Fusion Center Privacy Policy, web page," February 25, 2011. http://www.wv.gov/fusioncenter/Documents/West%20Virginia%20WVIFC%202-25-2011.pdf

Fusion centers were in their relatively nascent stages during development of the 2006 NIAC report, *Public-Private Sector Intelligence Coordination*. The report recommended that "government entities operate a national and State-level intelligence and information fusion capability focused on CIP." The report acknowledged that fusion centers would benefit the Intelligence Community as well as the public and private sectors through vetting requests for information, collaborative analysis, and timely dissemination of information across the full spectrum of CIP interests. Fusion centers should also develop, analyze, and disseminate intelligence at the lowest level possible of classification, with a strong bias toward open-source information, according to the report.

Recent assessments have generally found an improvement in the bi-directional information sharing between fusion centers and other levels of government, but have not addressed the intelligence requirements of the private sector. The Government Accountability Office's (GAO) report found that DHS is helping fusion centers develop capabilities but is lacking performance standards to effectively measure results. The GAO interviewed fusion centers that cited DHS grant funding as critical to achieving baseline capabilities. The GAO recommended that DHS define steps to develop and implement standard performance measures for centers and commit to a timeframe for completing them.[151] The report focused on the development of general baseline capabilities, not specifically on fusion center collaboration with the private sector.

The DHS Office of Inspector General (IG) noted the Department's progress in its efforts to improve information sharing with fusion centers. As a result of this improvement, the centers have successfully worked with DHS during large-scale events. However, the report found that DHS component collaboration in the information sharing process needs improvement, and that some intelligence products could better meet State and local needs. Fusion center personnel also make little use of information-sharing systems provided by DHS, according to the report. The IG report, however, focused on law enforcement and intelligence-information sharing and did not address the requirements of the private sector.[152]

On May 27, 2010, the President issued his *National Security Strategy*, which lays out a strategic approach for advancing the security of the American people. The *National Security Strategy* emphasizes the criticality of sharing information with the private sector to "integrate our approach to homeland security with our broader national security approach."[153] Both fusion centers and the private sector are recognized as integral pieces of the *National Security Strategy*. Accordingly, it seems appropriate that more focus should be placed on the continued improvement of information/intelligence sharing between fusion centers and the private sector.

In 2010, a Baseline Capabilities Assessment was performed - the first formal attempt to assess fusion center capabilities. This assessment enabled fusion centers to identify capability gaps and formulate short and long-term strategies to mitigate these gaps. According to this assessment: "80% of fusion centers have [at least some] procedures for information sharing and two-way communication with the private sector and critical infrastructure owners and operators." Also, to assist fusion centers with

[151] U.S. Government Accountability Office, "Information Sharing: Federal Agencies are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results," September 2010, http://www.gao.gov/new.items/d10972.pdf

[152] U.S. Department of Homeland Security, Office of Inspector General. *Information Sharing with Fusion Centers Has Improved, but Information System Challenges Remain*. October 2010. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_11-04_Oct10.pdf

[153] The White House, "National Security Strategy," May 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

analysis in the short-term, the *Critical Operational Capabilities for State and Major Urban Area Fusion Centers: Gap Mitigation Strategy*[154] stated that the Federal Government should sponsor attendance at the Critical Infrastructure and Key Resources Capabilities for Fusion Centers Workshop.

These represent significant efforts to increase the linkages between fusion centers and private sector owners and operators of critical infrastructure. Nonetheless, the level of engagement with the private sector remains dependent on the missions and intent of individual centers, which are determined by specific State and regional needs. While there are multiple models of success in this regard, including the eight success stories identified here, broader engagement remains dependent on jurisdictional needs rather than specific Federal guidance.

[154] Department of Homeland Security, "Critical Operational Capabilities for State and Major Urban Area Fusion Centers: Gap Mitigation Strategy." December 2010.

Appendix N. Examples of Effective Practices Cited in Case Studies

Introduction

The NIAC Intelligence Information Sharing Study interviewed more than 200 executives and subject matter experts from the Banking and Finance (B&F), Chemical (CHEM), Commercial Facilities (CF), Healthcare and Public Health (HPH), and Oil and Natural Gas (ONG) Sectors, as well as intelligence-community subject matter experts. These interviews revealed best practices that the public and private sectors are utilizing to effectively share information to make the decisions needed to guide critical investments, implement protective programs, and respond to infrastructure threats as they arise. The following effective practices were cited numerous times—often across sectors—as effective information-sharing mediums and initiatives:

- **Overseas Advisory Council (OSAC)**

  All five sectors cited the State Department-sponsored OSAC as an effective information-sharing platform. The OSAC acts as a liaison between the State Department security functions and the American private sector operating globally. This regular and timely sharing of information assists American companies in adapting to developments in the overseas security environment.

- **New York Police Department Shield (NYPD Shield)**

  The CF Sector cited NYPD Shield multiple times as a reliable and fast information-sharing resource. Unlike HSIN, NYPD Shield pushes information out to the private sector. It also has a training course functionality that is user-friendly and not as time-consuming as in-person courses.

- **International Security Management Association (ISMA)**

  ISMA was cited by three sectors as an excellent source of information. It includes security directors from Fortune 500 companies and is an avenue for networking and sharing of critical information across sectors.

- **Northern California Regional Intelligence Center (NCRIC)**

  The NCRIC was cited by both the CF Sector and the HPH Sector as a reliable and timely medium for disseminating information to the private sector. Its active engagement of the private sector included a briefing on what threats for the private sector to look out for leading up to the Fourth of July weekend.

- **Michigan Intelligence Operations Center (MIOC)**

  Both the HPH and the ONG Sectors cited the MIOC numerous times as being a leader in the sharing of relevant and timely information to Michigan's critical infrastructure owners and operators. The MIOC was identified and praised for its gathering of suspicious activity reports (SARs), analyzing the reports to deem their relevancy to Michigan's owners and operators, and disseminating this analysis to the private sector on a regular basis.

The following table identifies a variety of effective practices organized in terms of Associations, Fusion Centers, Products and Processes, and Information-Sharing Groups/Committees.

Table N: Case Studies Effective Practices Compilation

Title	Summary	Sectors
Associations		
American Chemistry Council (ACC) Security Committee	The committee meets 6 times a year and invites DHS to dialogue.	Chemical
American Gas Association (AGA) Security Committee	The committee has approximately 100 members representing 60 gas and utility companies. The committee is often on the receiving end of information from DHS.	ONG
American Petroleum Institute (API)	Consists of a very aggressive security subcommittee (cybernetics).	ONG
Calhospitalprepare.org	The California Hospital Association provides ongoing support to California's hospitals and health systems in all-hazard's disaster planning and response.	HPH
East Harris County Mutual Chemical Association	Mutual aid group that sends out notices of suspicious activity to participating organizations.	Chemical
International Security Management Association (ISMA)	Includes security directors from essentially Fortune 500 companies with mandatory meetings every 2 years—excellent for networking and sharing best practices.	Chemical, CF, HPH
Interstate Natural Gas Association (INGA)	INGA includes a cybersecurity working group that consists of subject matter experts across the sector.	ONG
Local Emergency Planning Commission (LEPC)	Provides a main information-sharing mechanism for local chemical companies.	Chemical
National Funeral Directors Association	Provides the primary information-sharing medium for funeral directors across the United States.	HPH
National Petroleum and Refiners Association (NPRA)	The NPRA has a Cyber Working Group, a Process Automation and Support Committee, and a Physical Security Committee. The cyber component is linked into all three.	ONG
Real Estate Roundtable	Roundtable serves as a conduit for members to share information on surveillance and suspicious activity and has direct point of contact with DHS sector-specialist.	CF (2)
Fusion Centers		
Arizona Counter-Terrorism Intelligence Center (ACTIC)	Identified as a best-practice fusion center for sharing information with the ONG Sector.	ONG
Boston Regional Intelligence Center (BRIC)	The local fusion center disseminates daily unclassified reports about incidents to its private-sector partners that include summaries on terrorism-related events, what to look out for, and suspicious activity.	CF
Houston Regional Intelligence Service Center	The ONG Sector collaborates closely with the Houston fusion center and has a long history of information sharing.	ONG
Indiana Intelligence Fusion Center	Identified as a fusion center that has a great relationship with its private-sector owners and operators.	ONG
Maryland Coordination and Analysis Center (MCAC)	The MCAC meets monthly with its State and local partners. It was suggested that this could be an even more effective practice if the meetings included the private sector.	Intelligence
Michigan Intelligence Operations Center (MIOC)	The MIOC collects and develops suspicious activity reports and situational awareness bulletins and disseminates them to key private-sector leadership.	HPH, ONG (Continued)

Table N: Case Studies Effective Practices Compilation (Continued)

Title	Summary	Sectors
New Jersey Regional Operations and Intelligence Center (ROIC)	The NJ ROIC provides a daily briefing to the CF Sector and often a direct link to the private sector.	CF, HPH
Northern California Regional Intelligence Center (NCRIC)	The NCRIC is a primary source of information for Northern California's owners and operators. For example, the center gave the private sector a briefing on what it should know leading up to the 4th of July holiday weekend.	CF (2), HPH
Palm Beach Regional Fusion Center (PBRFC)	The Chemical Sector interviewee identified PBRFC as a best-practice fusion center because it identified the 8 most relevant sectors for the region and created a cross-sector team that is invited to the center during any incident.	Chemical
Southern Nevada Counter Terrorism Center (SNCTC)	Hotels and casinos got together to fund an analyst to look at hotels and casinos – works full time in the fusion center and is responsive to those hotels and casinos – she's free labor because she's paid for by the industry.	Commercial Facilities
Virginia Fusion Center (VFC) and Tennessee Fusion Center (TFC) Copper Theft Coordination	Both the VFC and the TFC banded together to examine copper thefts for developing plans to improve security at affected facilities.	Chemical
Washington State Fusion Center	This fusion center was briefly cited as effectively incorporating public health into its operations.	HPH
West Virginia Fusion Center	Twice identified as a best-practice fusion center due to its ability to leverage State resources to perform outreach to the State's owners and operators.	ONG (2)
Products and Processes		
CFATS Help Desk	Serves as an excellent source from a regulatory standpoint for private-sector companies.	Chemical
DIBnet	An example of improved information sharing for defense industrial base (DIB), but closed to a small and exclusive group.	Intelligence
DHS Roll Call Release	*Roll Call Release* is a collaborative, For Official Use Only product produced by the DHS Office of Intelligence and Analysis and the FBI. The product is written specifically for State, local, and tribal "street-level" first responders, focusing on terrorist tactics, techniques, procedures, terrorism trends, and indicators of suspicious activity.	HPH
DOE *Energy Assurance Daily*	Provides a summary of open-source information concerning energy issues.	ONG
The Epidemic Information Exchange (Epi-X)	Epi-X is the Center for Disease Control's (CDC) web-based communications system for sharing information with public health officials. It provides rapid communications whenever there is a public health need.	HPH
NYPD Shield	NYPD is a public-private information sharing initiative that provides a central destination for private security managers to obtain information and engage NYPD resources.	CF (3)
ONG Classified Briefings	Semi-annual classified briefings to ONG SCC members that involve collaborative feedback on private-sector information needs.	ONG (Multiple citations) (Continued)

Table N: Case Studies Effective Practices Compilation (Continued)

Title	Summary	Sectors

University of Pittsburgh Center for Biosecurity	Shares information about chemical and biological threats that can be useful to the private sector.	CF
Homeland Security Information Network—Michigan (HSIN-MI)	The interviewee uses HSIN and HSIN-MI for finding information pertinent to the HPH Sector.	HPH
National Institute of Standards of Technology (NIST) e-mails	Regularly pushes e-mails on vulnerabilities and a source for information sharing to the private sector.	ONG
Texas Coastal Regional Advisory System (T-CRAS)	TCRAS is an information-sharing initiative run by the Houston JTTF to aid in the timely dissemination of information to law enforcement and the private sector during an emergency.	HPH
Travel Tracker	Software that enables companies to locate and message all of their travelers all over the world; particularly useful during emergency incidents.	Chemical
TrapWire	Vendor that takes a three-phased approach to risk assessments: 1) Identify red zones where terrorists would conduct surveillance 2) Provide tailored training that incorporates key players 3) Share SARs with other properties through a tailored software program.	CF
Sector Intelligence Needs (SINs) (ONG Sector)	The ONG sector has worked closely with DHS I&A to develop sector intelligence needs (SINs).	ONG (Multiple citations)
Information-Sharing Groups/Committees		
Asset Protection Executives (APEX)	Consists of a group of security directors in Chicago that meets once a month to share information and security concerns.	HPH
Hotel Security Working Group	This group started in June 2008 out of frustration from a lack of information sharing. Consists of global hotel companies and the State Department. The group meets twice a year to deal with global issues.	CF
HPH Sector Coordinating Council (HPH SCC) and SCC Conference Calls	Provides an avenue for the HPH private sector to share information, receive information from DHS and other Federal agencies, and jointly collaborate on analysis.	HPH
FBI Domestic Security Alliance Council (DSAC)	The DSAC is a strategic partnership between the FBI and the American private sector that enhances communications to promote the timely and effective exchange of information.	ONG
Illinois Terrorism Task Force (ITTF)	The ITTF is charged with the task of assuring that Illinois is ready to respond to an act of terrorism.	HPH
Lower Manhattan Security Initiative (LMSI)	The LMSI is designed to integrate public and private-sector security cameras and license-plate readers to supply critical information to a center monitored by police officers and public employees.	CF
Michigan CIP Committee	The CIP Committee has helped to recognize the relationships necessary for information sharing.	ONG (Continued)

Table N: Case Studies Effective Practices Compilation (Continued)

Title	Summary	Sectors
New Jersey Infrastructure Advisory Committee (IAC)	The IAC coordinates preparedness and information-sharing efforts with the critical infrastructure sectors represented on the IAC including Water, Energy, Nuclear, Defense Industrial Base, Information Technology and Communications, Transportation, Agriculture and Food, Healthcare and Public Health, and Chemical. Also represented are cross-sector cybersecurity, and the pharmaceutical and biotechnology industries.	HPH
South Central (PA) Task Force	Consists of 8 central Pennsylvania counties that have an “all-hazards” public-private mission that provides resources to communities when events exceed their capabilities.	HPH
U.S. Computer Emergency Readiness Team	US-CERT is the operational arm of the National Cyber Security Division at DHS and is a public-private partnership that is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local government, industry and international partners.	HPH
U.S. State Department’s Overseas Advisory Council (OSAC)	The OSAC has a mission to promote security cooperation between American private-sector interests worldwide and the State Department.	Chemical, CF (2), HPH, ONG

Appendix O. Sources

Adam, Nabil. *Workshop on Future Directions in Cyber-Physical Systems Security*. Washington, DC: U.S. Department of Homeland Security, Science and Technology Directorate, January 2010. http://www.ee.washington.edu/faculty/radha/dhs_cps.pdf.

Allard, William. “Asymmetric Warfare Against Oil and Natural Gas Infrastructure.” *The CIP Report* 7, no. 5 (2008): 4–5, 10. http://cip.gmu.edu/archive/CIPHS_TheCIPReport_November2008_OilandGas.pdf.

Allen, Charles E. “Keynote Address at the 2008 Annual International Association of Law Enforcement Intelligence Analysts and Law Enforcement Intelligence Unit Conference.” Boston, MA: April 8, 2008. http://www.dhs.gov/xnews/testimony/testimony_1207683448574.shtm.

Alperovitch, Dmitri. “Revealed: Operation Shady RAT,” McAfee White Paper. Santa Clara, CA: McAfee, 2011. http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

American Chemistry Council. *Making Strides to Improve Cyber Security in the Chemical Sector: 2009 Update*. Arlington, VA: American Chemistry Council ChemITC, March 2009. http://www.americanchemistry.com/s_chemitc/doc.asp?CID=1729&DID=6484.

Arizona Counter Terrorism Information Center. “Community Liaison Program.” The Arizona Department of Public Safety. http://www.azactic.gov/Community_Liaison/.

ASIS International Critical Infrastructure Working Group. *Critical Infrastructure Resource Guide 2009*. Alexandria, VA: ASIS International, 2009. http://www.asisonline.org/documents/downloadCIRG.xml?document=toolkit/cirg.pdf.

Assistant Secretary for Preparedness and Response. *From Hospitals to Healthcare Coalitions: Transforming Health Preparedness and Response in Our Communities*. Washington, D.C.: U.S. Department of Health and Human Services, May 2011. http://www.phe.gov/Preparedness/planning/hpp/Documents/hpp-healthcare-coalitions.pdf.

Baker, Stewart, Natalie Filiplak, and Katrina Timlin. *In the Dark: Crucial Industries Confront Cyber Attacks.* Santa Clara, CA: McAfee and the Center for Strategic and International Studies, April, 2011. http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf.

Baker, Stewart, Shaun Waterman, and George Ivanov. *In the Crossfire: Critical Infrastructure in the Age of Cyber War*. Washington, DC: McAfee and the Center for Strategic and International Studies, January 2010. http://img.en25.com/Web/McAfee/NA_CIP_RPT_REG_2840.pdf.

Barret, Devlin. “Nasdaq Acknowledges Security Breach.” *The Wall Street Journal*, February 6, 2011. http://online.wsj.com/article/SB10001424052748704843304576126370179332758.html.

Best, Richard. *Intelligence Information: Need-to-Know vs. Need-to-Share*. Washington, DC: Congressional Research Service, June 6, 2011. www.fas.org/sgp/crs/intel/R41848.pdf.

Best, Richard A., “Intelligence Issues for Congress,” Congressional Research Service Report RL33539. Washington, DC: Congressional Research Service, August 5, 2011.

Bond, Brandon. “Private Sector Partnership,” Presentation at the Northern California Regional Intelligence Center, San Francisco, December 10, 2009. http://www.tisp.org/index.cfm?pk=download&id=11941&pid=10261.

Boston Police Department. “Boston Police Department Virtual Community.” Boston Police Department. http://www.bpdnews.com/about/programs/.

BP. *Deepwater Horizon Containment and Response: Harnessing Capabilities and Lessons Learned*. London: BP, September 1, 2010. http://www.bp.com/liveassets/bp_internet/globalbp/globalbp_uk_english/incident_response/STAGING/local_assets/downloads_pdfs/Deepwater_Horizon_Containment_Response.pdf.

Bratton, William J. Speech given before the 2008 National Fusion Center Conference, San Francisco, March 2008. http://www.lapdonline.org/inside_the_lapd/content_basic_view/37865.

Burke, Tim and Dees Stribling. "Top Agencies Utilize State-of-the-Art Technology." *Public Safety IT Magazine*, November 2010. http://www.hendonpub.com/resources/articlearchive/details.aspx?ID=208133.

Carter, David L. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services, May 2009. http://www.cops.usdoj.gov/files/RIC/Publications/e050919201-IntelGuide_web.pdf.

Centers for Disease Control and Prevention, Office of Public Health Preparedness and Response, Biosurveillance Coordination Unit. *National Biosurveillance Strategy for Human Health, Version 2.0*. Washington, DC: U.S. Department of Health and Human Services, February 2010. http://www.cdc.gov/osels/pdf/NBSHH_V2_FINAL.PDF.

Centers for Disease Control and Prevention, Office of Public Health Preparedness and Response. *Public Health Preparedness Capabilities: National Standards for State and Local Planning*. Atlanta, GA: U.S. Department of Health and Human Services, March 2011. http://www.cdc.gov/phpr/capabilities/Capabilities_March_2011.pdf.

Center for Infrastructure Protection and Homeland Security. "Meeting the Threat of Terrorism: Information Sharing and a Virtual Reorganization of Government to Improve National Security." *The CIP Report* 8, no. 11 (2010): 4–5, 22. http://www.markle.org/sites/default/files/20100522_cip_report.pdf.

Center for Infrastructure Protection and Homeland Security, *The CIP Report* 9, no. 9 (2011). www-gs.llnl.gov/data/assets/docs/publications/2011-mar24_issue104_oil-gas.pdf.

Center for Strategic and International Studies. *A Threat Transformed: Al Qaeda and Associated Movements in 2011.* Washington, DC: Center for Strategic and International Studies, 2011. http://csis.org/files/publication/110203_Nelson_AThreatTransformed_web.pdf.

ChicagoFIRST. *ChicagoFIRST 2009 Annual Report*. Chicago: ChicagoFIRST, March 2010. https://www.chicagofirst.org/resources/2009_annual_report.pdf.

Clausing, Jeri. "Hotel Companies Band Together to Share Security Information." *Travel Weekly*, February 15, 2011. http://www.travelweekly.com/Travel-News/Hotel-News/Hotel-companies-band-together-to-share-security-information/?a=hotels.

Coe, Michael. *To Investigate the Practice and Implementation of Designing out Crime and the Use and Effectiveness of Closed Circuit Television (CCTV) in Public Places*. Canberra, Australia: The Winston Memorial Trust of Australia, 2008. http://www.churchilltrust.com.au/site_media/fellows/Coe_Michael_2008.pdf.

Colorado Information Analysis Center. *Infrastructure Protection Threat Report: Chemical Sector*. Lakewood, CO: Colorado Information Analysis Center, 2010. http://denvergov.org/Portals/428/documents/CIAC-Threat%20Report%20Chemical%20Sector.pdf.

Commonwealth Fusion Center. *Commonwealth Fusion Center*. Maynard, MA: Commonwealth Fusion Center. http://www.mass.gov/Eeops/docs/msp/homeland_security/terrorism/fusion_center/fusion-center-brochure.pdf.

Critical Infrastructure Information Act of 2002, 6 U.S.C. Sections 131–134 (November 25, 2002). http://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf.

Critical Infrastructure Partnership Advisory Council. *2010 Critical Infrastructure Partnership Advisory Council Annual*. Washington, DC: U.S. Department of Homeland Security, 2010. http://www.dhs.gov/xlibrary/assets/cipac/cipac-annual-2010.pdf.

Critical Infrastructure Partnership Advisory Council. "Council Members, Critical Infrastructure Partnership Advisory Council." U.S. Department of Homeland Security. http://www.dhs.gov/files/committees/editorial_0848.shtm#7.

Dallas Police Department. "IWatch Dallas, Do You?" Dallas: Dallas Police Department. http://www.dallaspolice.net/content/11/66/uploads/dpd091510dp02_smaller.pdf.

Davis, Robert C., Christopher Ortiz, Robert Rowe, Joseph Broz, George Rigakos, and Pam Collins. *An Assessment of the Preparedness of Large Retail Malls to Prevent and Respond to Terrorist Attack*. Washington, DC: Police Foundation, 2006. http://www.ncjrs.gov/pdffiles1/nij/grants/216641.pdf.

Elsea, Jennifer K. *The Protection of Classified Information: The Legal Framework*. Washington, DC: U.S. Congressional Research Service, January 10, 2011. http://www.fas.org/sgp/crs/secrecy/RS21900.pdf.

Executive Order No. 2005-22, "Establishing the Governor's Executive Oversight Committee of the Arizona Counter-Terrorism Information Center and Reporting Channels" (2005). http://www.azdohs.gov/Documents/ACTIC/EO2005-22.pdf.

Executive Order No. 12,333, 3 Code of Federal Regulations 200 (December 4, 1981). http://www.fas.org/irp/offdocs/eo12333.htm.

Executive Order No. 13,228, 66 Federal Register 51,812 (October 8, 2001). http://www.fas.org/irp/offdocs/eo/eo-13228.htm.

Executive Order No. 13,284, 68 Federal Register 4,075 (January 23, 2003). http://www.fas.org/irp/offdocs/eo/eo-13284.htm.

Executive Order No. 13,311, 68 Federal Register 45,149 (July 29, 2003). http://www.fas.org/irp/offdocs/eo/eo-13311.htm.

Executive Order No. 13,355, 69 Federal Register 53,593 (August 27, 2004). http://www.fas.org/irp/offdocs/eo/eo-13355.htm.

Executive Order No. 13,388, 70 Federal Register 62,023 (October 25, 2005). http://www.fas.org/irp/offdocs/eo/eo-13388.htm.

Executive Order No. 13,470, 73 Federal Register 45,325 (July 30, 2008). http://www.fas.org/irp/offdocs/eo/eo-13470.htm.

Executive Order No. 13,529, 75 Federal Register 3331 (January 21, 2010). http://ra.defense.gov/documents/rtm/EO%2013529%20-%20Haiti.pdf.

Executive Order No. 13,556, 75 Federal Register 68,675 (November 4, 2010). http://www.fas.org/irp/offdocs/eo/eo-13556.htm.

Federal Emergency Management Agency (FEMA). *Critical Infrastructure and Key Resources Support Annex*. Washington DC: FEMA, January 2008. http://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf.

Financial Services Information Sharing and Analysis Center. *Cyber Attack against Payment Processes Exercise: 2010 CAPP Exercise Executive Summary*. Sterling, VA: Financial Services Information Sharing and Analysis Security Operations Center, 2010. http://www.fsisac.com/files/public/db/p243.pdf.

Financial Services Sector Coordinating Council (FSSCC) and Financial and Banking Information Infrastructure Committee (FBIIC). *Roadmap for Improved Information Sharing*. Washington, DC: FSSCC and FBIIC Cyber Security Intelligence and Information Sharing Workgroups, December 2008. http://www.whitehouse.gov/files/documents/cyber/FSSCC-FBIIC%20-%20ROADMAP%20FOR%20IMPROVED%20INFORMATION%20SHARING.pdf.

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. *Annual Report*. Financial Services Sector Coordinating Council, 2009. https://www.fsscc.org/fsscc/reports/2010/FSSCC-2009AnnualReport.pdf.

Florida Department of Law Enforcement. “Investigations and Forensic Science Program Office: Office of Statewide Intelligence.” Florida Department of Law Enforcement. http://www.fdle.state.fl.us/content/getdoc/595aab23-67a2-4dd8-9bdb-e0dac2f25559/OSI-Home.aspx.

Franco, Crystal and Mary Beth Hansen. “The State of Biopreparedness: Lessons from Leaders, Proposals for Congress.” *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 8, no. 4 (2010): pp. 379–384. http://www.upmc-biosecurity.org/website/resources/publications/2010/pdf/2010-12-10-state_of_bioprep.pdf.

Gallagher, Sean. “Cyber Commands Puts its Philosophy Into Action.” *Federal Computer Week*, November 10, 2010. http://fcw.com/articles/2010/11/17/cyber-defense-year-in-review-analysis.aspx.

Georgia Information Sharing and Analysis Center. “GISAC Open Source Reports: Weekly Open Source Reports.” Georgia Information Sharing and Analysis Center. http://www.gema.ga.gov/rss_generator.nsf/rss?openagent&uid=ECEED88516495948852575640066DE25.

German, Michael and Jay Stanley. *What’s Wrong With Fusion Centers?* Washington, DC: American Civil Liberties Union, December 2007. http://www.aclu.org/technology-and-liberty/whats-wrong-fusion-centers-executive-summary.

Ginsberg, Wendy R. *CRS Issue Statement on Government Information: Access and Protection*. Washington, DC: Congressional Research Service, January 13, 2010.

Ginsberg, Wendy R. *The Obama Administration’s Open Government Initiative: Issues for Congress*. Washington, DC: Congressional Research Service, January 28, 2011. http://www.fas.org/sgp/crs/secrecy/R41361.pdf.

Global Justice Information Sharing Initiative. *Baseline Capabilities for State and Major Urban Area Fusion Centers*. Washington, DC: U.S. Department of Homeland Security and U.S. Department of Justice, September 2008. http://www.it.ojp.gov/documents/baselinecapabilitiesa.pdf.

Government of Canada*. Canada’s Cyber Security Strategy: For a Stronger and More Prosperous Canada,* 2010. http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf.

Hall, Stacy, Lou Marciani, and Walter Cooper. “Sport Venue Security: Planning and Preparedness for Terrorist-Related Incidents.” *The SMART Journal* 4, no. 2 (2008): pp.6–15. http://www.thesmartjournal.com/venues.pdf.

Hatcher, Monica. “Only a Handful of Huston Plants Checked For Safety Standards.” *Houston Chronicle*, April 5, 2010. http://www.chron.com/disp/story.mpl/business/energy/6943880.html.

Hearing before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. 109th Cong. (November 17, 2005) (statement of Melissa Smislova, Acting Director, Department of Homeland Security, Homeland Infrastructure Threat and Risk Analysis Center). http://ftp.resource.org/gpo.gov/hearings/109h/35939.txt.

Hearing before the Senate Committee on Homeland Security and Governmental Affairs. 111th Cong. (January 8, 2009) (statement of Charles E. Allen, Under Secretary for Intelligence and Analysis, Department of Homeland Security). http://hsgac.senate.gov/public/_files/010809Allen.pdf.

Hearing on Cyber Security and Data Protection in the Financial Sector, Before the Senate Committee on Banking, Housing, and Urban Affairs. 112th Cong. (June 21, 2011) (Statement of Mr. Pablo A. Martinez, Deputy Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service). http://www.dhs.gov/ynews/testimony/20110621-martinez-cyber-crime.shtm.

Hearing on Department of Homeland Security National Programs and Protection Directorate, Before the House Committee on Energy and Commerce. 112th Cong. (March 30, 2011) (testimony of Rand Beers, Directorate Under Secretary of the U.S. Department of Homeland Security National Programs and Protection). http://www.dhs.gov/ynews/testimony/testimony_1301517368947.shtm.

Hearing on Examining the Cyber Threat to Critical Infrastructure and the American Economy, *Before the Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies*, 112th Cong. (March 16, 2011) (testimony of Philip Reitinger, Deputy Under Secretary of the National Protection and Programs Directorate). http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Reitinger.pdf.

Hearing on Hacked Off: Helping Law Enforcement Protect Private Financial Information, Before the House Committee on Financial Services. 112th Cong. (June 29, 2011) (Testimony of Assistant Director A.T. Smith, Office of Investigations, U.S. Secret Service). http://www.dhs.gov/ynews/testimony/20110629-smith-protecting-financial-information.shtm.

Hearing on Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration, Before the Committee on Homeland Security and Governmental Affairs. 112th Cong. (March 10, 2011). http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=0c531692-c661-453a-bc97-654be6eb7d00.

Hearing on Preventing Chemical Terrorism: Building a Foundation of Security at Our Nation’s Chemical Facilities, Before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. 112th Cong. (February 11, 2011) (testimony of Rand Beers, Directorate Under Secretary of U.S. Department of Homeland Security, National Programs and Protection). http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Beers_1.pdf.

Hearing on Protecting Cyberspace: Assessing the White House Proposal, Before the Homeland Security and Governmental Affairs Committee. 112th Cong. (May 23, 2011) (testimony of Philip Reitinger, Deputy Under Secretary of the National Protection and Programs Directorate). http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=96EF8175-E114-4FE0-AB31-B42D45D599AC.

Hearing on Sharing and Analyzing Information to Prevent Terrorism, Before the Committee on the Judiciary. 111th Cong. (March 24, 2010) (written testimony by Zöe Baird and Slade Gorton). http://judiciary.house.gov/hearings/printers/111th/111-116_55598.PDF .

Hearing on Taking Measures of Countermeasures (Part 1), Before the Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications. 112th Cong. (April 13, 2011) (testimony of Segaran Pillaim, Chief Medical and Science Advisor).

Hearing on Ten Years after 9/11: A Report from the 9/11 Commission, *Before the Committee on Homeland Security and Governmental Affairs*. 112th Cong. (March 30, 2011). http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=759EFC68-191F-4DFD-B362-C3197C6CB624.

Hearing on the Department of Homeland Security Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure, *Before the Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies*. 112th (April 15, 2011) (written statement of Jane Carlin, on behalf of the Financial Services Sector Coordinating Council). http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Carlin_0.pdf.

Hearing on the Department of Homeland Security Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure, Before the Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. 112th Cong. (April 15, 2011) (testimony of Seán P. McGurk, Director of the National Cybersecurity and Communications Integration Center, National Protection and Programs Directorate). http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20McGurk.pdf.

Hearing on the Department of Homeland Security Intelligence Enterprise - Past, Present, and Future, Before the Subcommittee on Counterterrorism and Intelligence House Committee on Homeland Security. 112th Cong. (June 1, 2011) (Statement for the Record of Caryn A. Wagner, Under Secretary and Chief Intelligence Officer, Office of Intelligence and Analysis). http://www.dhs.gov/ynews/testimony/testimony_1306937528609.shtm.

Hearing on Understanding the Homeland Threat Landscape—Consideration for the 112th Congress, Before the Committee on Homeland Security. 112th Cong. (February 9, 2011) (testimony of Janet Napolitano, Secretary). http://homeland.house.gov/sites/homeland.house.gov/files/02.09.11%20Sec.%20Napolitano%20Testimony.pdf.

Hibbard, Paul J. *U.S. Energy Infrastructure Vulnerability: Lessons from the Gulf Coast Hurricanes*. Boston: Analysis Group, March 2006. http://www.bipartisanpolicy.org/library/report/us-energy-infrastructure-vulnerability-lessons-gulf-coast-hurricanes.

Higgins, Kelly Jackson. “Hospitality Industry Hit Hardest by Hacks.” *Dark Reading*, February 4, 2010. http://www.darkreading.com/database-security/167901020/security/attacks-breaches/222601178/hospitality-industry-hit-hardest-by-hacks.html.

Homeland Security Committee. *Razing Expectations: Erecting a Strategic Vision for Fusion Centers*. Alexandria, VA: International Association of Chiefs of Police, January 19, 2010. http://www.theiacp.org/LinkClick.aspx?fileticket=A%2b72iBFNpLw%3d&tabid=87.

Homeland Security Act of 2002, Public Law 107-296 (November 25, 2002). http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.

Homeland Security Presidential Directive 5: Management of Domestic Incidents (February 28, 2003). http://www.dhs.gov/xabout/laws/gc_1214592333605.shtm.

Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (December 17, 2003). http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

Homeland Security Presidential Directive 21: Public Health and Medical Preparedness (October 18, 2007). http://www.dhs.gov/xabout/laws/gc_1219263961449.shtm#1.

Honeywell Process Solutions. *Maritime Security: Meeting Threats to the Offshore Oil and Gas Industry*. Phoenix: Honeywell Process Solutions, May 2008. http://hpsweb.honeywell.com/NR/rdonlyres/712E28C2-85D7-4BDD-A9DB-0A09330F32C2/63840/Maritime_Securty_WhitePaper.pdf.

Hotel News Resource. "AH and LA, DHS Launch Security, Terrorism Awareness Initiative." *Hotel News Resource*, November 16, 2010. http://www.hotelnewsresource.com/article50228.html.

Hurst, Cindy. *The Terrorist Threat to Liquefied Natural Gas: Fact or Fiction*. Washington, DC: Institute for the Analysis of Global Security, February 2008. http://www.iags.org/hurstlng0208.pdf.

IBM. *IBM X-Force 2010 Trend and Risk Report*. Somers, NY: IBM X-Force Team, March 2011. https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-spsm-tiv-sec-wp&S_PKG=IBM-X-Force-2010-Trend-Risk-Report.

IBM. *Meeting the Cybersecurity Challenge: Empowering Stakeholders and Ensuring Coordination*. Somers, NY: IBM, February 2010. http://www.homelandcouncil.org/pdfs/cyber_whitepaper_ibm.pdf.

Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53 (August 3, 2007). http://intelligence.senate.gov/laws/pl11053.pdf.

Institute of Medicine of the National Academies. *Biowatch and Public Health Surveillance: Evaluating Systems for the Early Detection of Biological Threats*. Washington, DC: Institute of Medicine of the National Academies, December 2009. http://www.iom.edu/~/media/Files/Report%20Files/2009/BioWatch-Public-Health-Surveillance/Biowatch%20and%20Public%20Health%20Surveillance%202009%20%20Report%20Brief.ashx.

Intelligence and National Security Alliance and Homeland Security Intelligence Council. *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*. Arlington, VA: Intelligence and Nation Security Alliance, September 2011. https://images.magnetmail.net/images/clients/INSA/attach/INSA_Homeland_Security_Intelligence.pdf.

Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458 (December 17, 2004). http://intelligence.senate.gov/laws/pl108-458.pdf.

Interagency Threat Assessment and Coordination Group. *Intelligence Guide for First Responders*. Washington, DC: Office of the Director of National Intelligence, U.S. Department of Homeland Security, Federal Bureau of Investigation, and the National Counterterrorism Center, March 2011. http://www.ise.gov/sites/default/files/ITACG_Guide_2ed.pdf.

Jackson, James K. *Foreign Investment and National Security: Economic Considerations*. Washington, DC: U.S. Congressional Research Service, March 10, 2011. http://www.fas.org/sgp/crs/natsec/RL34561.pdf.

Jackson, James K. *Foreign Investment, CFIUS, and Homeland Security: An Overview*. Washington, DC: U.S. Congressional Research Service, March 30, 2011. http://www.fas.org/sgp/crs/homesec/RS22863.pdf.

Jackson, James K. *The Committee on Foreign Investment in the United States (CFIUS)*. Washington, DC: U.S. Congressional Research Service, March 30, 2011. http://assets.opencrs.com/rpts/RL33388_20110330.pdf.

Jackson, James K. *The Financial Action Task Force: An Overview*. Washington, DC: U.S. Congressional Research Service, February 1, 2011. http://www.fas.org/sgp/crs/misc/RS21904.pdf.

Johnson, Bart. "Fusion Centers: Engaging Law Enforcement in the Nation's Homeland Security Enterprise." *Sherriff Magazine,* March/April 2011. http://www.ourdigitalmags.com/display_article.php?id=658612.

Kaplan, Eben. *Targets for Terrorists: Chemical Facilities*. Washington, DC: Council on Foreign Relations, December 11, 2006. http://www.cfr.org/united-states/targets-terrorists-chemical-facilities/p12207?breadcrumb=%2Fissue%2F452%2Ftargets_for_terrorists.

Keyer, Doug and Lehew W. Miller III. "Nationwide SAR Initiative Delivers Value to Fusion Centers." *The Police Chief Magazine*, February 2011. http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=2311&issue_id=22011.

Kosal, Margaret. *Terrorism Targeting Industrial Chemical Facilities: Strategic Motivations and the Implications for U.S. Security*. Stanford, CA: Stanford University, Center for International Security and Cooperation, 2005. http://cstsp.aaas.org/files/kosal_terrorist%20attacks%20on%20chemical%20infrastructure_sct.pdf.

Kosar, Kevin R. *Classified Information Policy and Executive Order 13526*. Washington, DC: U.S. Congressional Research Service, December 10, 2010. http://www.fas.org/sgp/crs/secrecy/R41528.pdf.

LaTourrette, Tom, David R. Howell, David E. Mosher, and John MacDonald. *Reducing Terrorism Risk at Shopping Centers: An Analysis of Potential Security Options*. Santa Monica, CA: Rand Corporation, 2006. http://www.rand.org/pubs/technical_reports/2006/RAND_TR401.pdf.

Lavigne, Paula. "Officials Ramp Up Stadium Security." *ESPN.com*, February 3, 2010. http://sports.espn.go.com/nfl/playoffs/2009/news/story?id=4882618.

Lee, Gwanhoo and Young Hoon Kwak. *An Open Government Implementation Model: Moving to Increased Public Engagement*. Washington, DC: IBM Center for the Business of Government, 2010. http://www.businessofgovernment.org/sites/default/files/An%20Open%20Government%20Implementation%20Model.pdf.

Lumension. *Federal Cyber Security Outlook for 2010*. Scottsdale, AZ: Lumension Security, Inc., March 2010. http://www.lumension.com/Federal-Cyber-Security-Outlook-for-2010.aspx.

Markle Foundation. *Markle Foundation Task Force on National Security in the Information Age*. New York: Markle Foundation, October 2008. http://www.markle.org/sites/default/files/markletaskforce_oct2008.pdf.

Markle Foundation. *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trust Information Sharing Environment*. New York: Markle Foundation. July 1, 2006. http://www.markle.org/sites/default/files/2006_nstf_report3.pdf.

Markle Foundation. *Nation at Risk: Policy Makers Need Better Information to Protect the Country*. New York: Markle Foundation, March 2009. http://www.markle.org/sites/default/files/20090304_mtf_report.pdf.

Markle Foundation. *Reforming the Culture of National Security: Vision, Clarity, and Accountability*. New York: Markle Foundation and the New York University School of Law Center on Law and Security, April 2009. http://www.markle.org/sites/default/files/20090403_reforming_culture_natsec.pdf.

Markle Foundation Task Force on National Security in the Information Age. *Meeting the Threat of Terrorism: Authorized Use*. New York: Markle Foundation, August 1, 2009. http://www.markle.org/sites/default/files/20090825_authusestndrd.pdf.

Markle Foundation Task Force on National Security in the Information Age. *Meeting the Threat of Terrorism: Culture Change*. New York: Markle Foundation, September 1, 2009. http://www.markle.org/sites/default/files/20090825_culturechange.pdf.

Markle Foundation Task Force on National Security in the Information Age. *Meeting the Threat of Terrorism: Discoverability*. New York: Markle Foundation, September 1, 2009. http://www.markle.org/sites/default/files/20090825_discoverability.pdf.

Maryland Governor's Office of Homeland Security. "Vulnerability Assessment." State of Maryland. http://www.gohs.maryland.gov/va_accomplishments.html.

Masse, Todd, Siobhan O'Neil, and John Rollins. *Fusion Centers: Issues and Options for Congress*. Washington, DC: U.S. Congressional Research Service, July 6, 2007. http://epic.org/privacy/fusion/crs_fusionrpt.pdf.

Maxwell School of Syracuse University. *Chemical Security in New Jersey: An Overview of Planning, Information Sharing, and Response*. Syracuse, NY: Maxwell School of Syracuse University, June 11, 2007. http://insct.syr.edu/uploadedFiles/insct/uploadedfiles/PDFs/Chemical%20Security%20in%20New%20Jersey.pdf.

McAfee Foundstone Professional Services and McAfee Labs. *Global Energy Cyberattacks: "Night Dragon."* Santa Clara, CA: McAfee, February 2011. http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

McDaniel, Michael, Emad (Al) Shenouda, and M. John Bustria. "The Functional Desks as Collaborative Mechanisms in the Michigan Intelligence Operations Center." *Homeland Security Affairs*, Supplement No. 2, 2008. http://www.hsaj.org/?special:fullarticle=supplement.2.4.

McKay, Jim and Elaine Pittman. "Las Vegas Fusion Center Is a Model for Public-Private Collaboration." *Emergency Management*, May 24, 2011. http://www.emergencymgmt.com/safety/Las-Vegas-Fusion-Center-Public-Private-Collaboration-052411.html.

Mehdizadeh, Yahya. "Securing Oil and Gas Assets." *Hydrocarbon World* 3, no. 2 (2008): pp.34–37. http://www.touchgroupplc.com/pdf/3231/mehdizadeh.pdf.

Michigan Intelligence Operations Center. "Critical Infrastructure Protection (CIP) Desk." Michigan Intelligence Operations Center. http://www.michigan.gov/mioc/0,1607,7-241-55994---,00.html.

Michigan Intelligence Operations Center. "Monthly CIKR Monitor." *CIKR Monitor*, August2010.

Monahan, Lt. Tom. "Safeguarding America's Playground." *University of Nevada Las Vegas Institute for Security Studies*, July/August 2010.

Morrison, Alan D. and William J. Wilhelm, Jr. "Investment Banking: Past, Present, and Future," *Journal of Applied Corporate Finance* 19, no. 1 (winter 2007). http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6622.2007.00124.x/abstract.

Moteff, John D. *Critical Infrastructures: Background, Policy, and Implementation*. Washington, DC: U.S. Congressional Research Service, June 7, 2010. http://www.fas.org/sgp/crs/homesec/RL30153.pdf.

Moteff, John D. *CRS Issue Statement on Critical Infrastructure Security*. Washington, DC: U.S. Congressional Research Service, January 12, 2010. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA514725.

Mullen, Erin and Briana Stephan. "Homeland Security Information Network: An Online Information-Sharing Tool for the Healthcare and Public Health Sector." Presentation given at the 2011 Public Health Preparedness Summit, February 24, 2011. http://www.phprep.org/2011/Agenda/upload/Homeland-Security-Information-Network-An-Online-Information-Sharing-Tool.pdf.

Nanto, Dick. *Economics and National Security: Implications for U.S. Policy*. Washington, DC: U.S. Congressional Research Service, January 4, 2011. http://www.fas.org/sgp/crs/natsec/R41589.pdf.

National Council of Information Sharing and Analysis Centers. "The Role of Information Sharing and Analysis Centers (ISACs) in Private/Public Sector Critical Infrastructure Protection." National Council of Information Sharing and Analysis Centers, January 2009. http://www.isaccouncil.org/index.php?option=com_docman&task=cat_view&gid=40&Itemid=208.

National Cyber Defense Initiative. Financial Services Workshop Report: "Helping Form a Sound Investment Strategy to Defend against Strategic Attack on Financial Services." Washington, DC: National Science Foundation and Department of Homeland Security Science and Technology, February 4, 2010. http://ncdi.cisr.us/FI_Workshop_Report_100204.pdf.

National Infrastructure Advisory Council. *A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council*. Washington, DC: National Infrastructure Advisory Council, October 19, 2010. http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf.

National Infrastructure Advisory Council. *Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations.* Washington, DC: U.S. Department of Homeland Security, October 14, 2008. http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf.

National Infrastructure Advisory Council. *Optimization of Resources for Mitigating Infrastructure Disruptions Study*. Washington, DC: U.S. Department of Homeland Security, October 19, 2010. http://www.dhs.gov/xlibrary/assets/niac/niac-optimization-resources-final-report-10192010.pdf.

National Infrastructure Advisory Council. *Public-Private Sector Intelligence Coordination: Final Report and Recommendations By The Council.* Washington, DC: U.S. Department of Homeland Security, June 11, 2006. http://www.dhs.gov/xlibrary/assets/niac/niac_icwgreport_july06.pdf.

National Infrastructure Advisory Council. *The Insider Threat to Critical Infrastructure*. Washington, DC: U.S. Department of Homeland Security, April 8, 2008. http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.

National Petroleum Council*. Securing Oil and Natural Gas Infrastructures in the New Economy*. Washington, DC: National Petroleum Council, June 2001. http://www.npc.org/reports/NPC_CIP_4.pdf.

National Security Cyberspace Institute. *Cyber Pro* 4, no. 4 (February 24, 2011). http://www.nsci-va.org/SeniorLeaderPerspectives/2011-02-CyberPro-Stewart%20Baker.pdf.

National Security Institute. "Educate employees about security easily and cost-effectively with Employee Security Connection." National Security Institute. http://www.nsi.org/esc-top-breaches.html.

National Security Preparedness Group. *Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations*. Washington, DC: Bipartisan Policy Center, September 2011. http://www.bipartisanpolicy.org/sites/default/files/CommissionRecommendations.pdf.

Nelson, Rick and Thomas M. Sanderson. *A Threat Transformed: Al Qaeda and Associated Movements in 2011*. Washington, DC: Center for Strategic and International Studies, 2011. http://csis.org/publication/threat-transformed.

North Dakota State and Local Intelligence Center. *North Dakota Homeland Security Anti-Terrorism Summary*. Bismarck, ND: North Dakota State and Local Intelligence Center, February 22, 2011. http://www.nd.gov/des/uploads/resources/569/nd-all-source-anti-terrorism-02-22-2011.pdf.

Northern California Regional Intelligence Center home page. https://ncric.org/(X(1)S(qyj4go55bl02pu3mcbdohprv))/default.aspx?AspxAutoDetectCookieSupport=1.

Office of Electricity Delivery and Energy Reliability. "Energy Assurance Daily." U.S. Department of Energy. http://www.oe.netl.doe.gov/ead.aspx.

Office of Electricity Delivery and Energy Reliability. "ISERnet Login." U.S. Department of Energy. https://www.oe.netl.doe.gov/ISERNET/login.aspx.

Office of Infrastructure Protection. *The CIKR Information Sharing Environment*. Washington, DC: U.S. Department of Homeland Security, January 9, 2009.

Office of Inspector General. *Information Sharing With Fusion Centers Has Improved, but Information System Challenges Remain*, OIG-11-04. Washington, DC: U.S. Department of Homeland Security, October 2010. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_11-04_Oct10.pdf.

Office of Inspector General. *Protective Security Advisor Program Efforts to Build Effective Critical Infrastructure Partnerships: Oil and Natural Gas Subsector*. Washington, DC: U.S. Department of Homeland Security, November 2010. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_11-12_Nov10.pdf.

Office of Intelligence and Analysis. "DHS Open Source Enterprise Daily Cyber Report." Washington, DC: U.S. Department of Homeland Security, March 2, 2011.

Office of Intelligence and Analysis. *Strategic Plan Fiscal Year 2011–Fiscal Year 2018*. Washington, DC: Department of Homeland Security, February 2011. http://www.dhs.gov/xlibrary/assets/ia-fy2011-fy2018-strategic-plan.pdf

Office of Intelligence. *(U) Pipeline Threat Assessment*. Washington, DC: U.S. Transportation Security Administration, January 18, 2011.

http://www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1101TSAModalThreatAssessment.pdf.

Office of Risk Management and Analysis. *Risk Management Practices in the Public and Private Sector: Executive Summary*. Washington, DC: U.S. Department of Homeland Security, September 2010. https://www.llis.dhs.gov/docdetails/details.do?contentID=49145.

Office of the Director of National Intelligence. *National Intelligence: A Consumer's Guide – 2009*. Washington, DC: Office of the Director of National Intelligence, 2009. http://www.dni.gov/IC_Consumers_Guide_2009.pdf.

Office of the Director of National Intelligence. *The National Intelligence Strategy of the United States of America.* Washington, DC: Office of the Director of National Intelligence, August 2009. http://www.dni.gov/reports/2009_NIS.pdf.

Office of the Director of National Intelligence. *United States Intelligence Community Information Sharing Strategy.* Washington, DC: Office of the Director of National Intelligence, February 22, 2008. http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf.

Office of the Press Secretary. "Fact Sheet: Cybersecurity Legislative Proposal." White House, May 12, 2011. http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

Office of the Press Secretary. "Memorandum from the President for the Heads of Executive Departments and Agencies, Subject: Guidelines and Requirements in Support of the Information Sharing Environment (ISE)." Washington, DC: White House, December 16, 2005. http://www.fas.org/sgp/news/2005/12/wh121605-memo.html.

Office of the Press Secretary. "Secretary Napolitano Announces Expansion of 'If You See Something, Say Something' Campaign to Walmart Stores Across the Nation." December 6, 2010. http://www.dhs.gov/ynews/releases/pr_1291648380371.shtm.

O'Neil, Siobhan. "The Relationship between the Private Sector and Fusion Centers: Potential Causes for Concern and Realities." *Homeland Security Affairs*, Supplement No. 2, 2008. http://www.hsaj.org/?special:fullarticle=supplement.2.7.

Parfomak, Paul W. *Keeping America's Pipelines Safe and Secure: Key Issues for Congress*. Washington, DC: U.S. Congressional Research Service, March 17, 2011. http://www.fas.org/sgp/crs/homesec/R41536.pdf.

Parfomak, Paul W. *Pipeline Safety and Security: Federal Programs*. Washington, DC: U.S. Congressional Research Service, February 2008. http://www.fas.org/sgp/crs/homesec/RL33347.pdf.

Parfomak, Paul W. and Adam Vann. *Liquefied Natural Gas (LNG) Import Terminals: Siting, Safety, and Regulation*. Washington, DC: U.S. Congressional Research Service, December 14, 2009. http://www.fas.org/spp/civil/crs/RL32205.pdf.

Partnership for Public Service. *Securing the Future: Management Lessons of 9/11*. McLean, VA: Booze Allen Hamilton, August 2011, http://www.ourpublicservice.org/OPS/publications/viewcontentdetails.php?id=164

Paulk, Mark C., Charles V. Weber, and Mary B. Chrissis. *The Capability Maturity Model: A Summary*, paper 2. Pittsburg, PA: Carnegie Mellon University, 1999.

"Payments Processing Information Sharing Council Forms to Foster Information Sharing Among Payments Processors." Financial Services Information Sharing and Analysis Center, March 23, 2009. http://www.fsisac.com/files/public/db/p173.pdf.

Priest, Dana and William H. Arkin. “Monitoring America.” *The Washington Post*, December 20, 2010. http://projects.washingtonpost.com/top-secret-america/articles/monitoring-america/print/.

Pritchett, Beverly A. *Thesis: A Prescription for Developing a Quality Health Threat Assessment*. Monterrey, CA: Naval Postgraduate School, December 2008. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA493974.

Process-Performance Improvement Consultants, AGA Natural Gas Security Committee, and INGAA Security Committee. *Security Practices Guidelines Natural Gas Industry Transmission and Distribution*. Washington DC: American Gas Association and Interstate Natural Gas Association of America, revised May 2008. http://www.aga.org/membercenter/gotocommitteepages/NGS/Documents/0805SECGUIDELINES.pdf.

Program Manager, Information Sharing Environment. *Annual Report to Congress*. Washington DC: Information Sharing Environment, July 2010. http://www.ise.gov/sites/default/files/ISE_AR-2010_Final_2010-07-29.pdf.

Program Manager, Information Sharing Environment. *Information Sharing Environment Implementation Plan*. Washington, DC: Office of the Director of National Intelligence, November 2006. http://www.ise.gov/sites/default/files/ise-impplan-200611_0.pdf.

Project on National Security Reform. *Forging a New Shield*. Arlington, VA: Project on National Security Reform, November 2008. http://www.pnsr.org/data/files/pnsr_forging_a_new_shield_report.pdf.

Public Safety Committee. “Dallas Police Department Fusion Center Update, Metro Operations Support and Analytical Intelligence Center.” Presentation by the Dallas Police Department, June 15, 2009. http://www.dallascityhall.com/committee_briefings/briefings0609/PS_Fusion_Center_061509.pdf.

RAND National Defense Research Institute. *What Should Be Classified? A Framework with Application to the Global Force Management Data Initiative*. Santa Monica, CA: RAND Corporation, 2010. http://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG989.pdf.

Randol, Mark A. *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress*, R40602. Washington, DC: U.S. Congressional Research Service, May 27, 2009. http://epic.org/crs-rept_dhs-oversight.pdf.

Randol, Mark A. *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress*. Washington, DC: U.S. Congressional Research Service, March 19, 2010. http://www.fas.org/sgp/crs/homesec/R40602.pdf.

Ratner, Michael. *Global Natural Gas: A Resource*. Washington, DC: U.S. Congressional Research Service, December 22, 2010. http://www.fas.org/sgp/crs/misc/R41543.pdf.

Real Estate Roundtable. *2010 Annual Report*. Washington, DC: Real Estate Roundtable, 2010. http://www.rer.org/Advocacy/2010_Annual_Report.aspx.

Reitinger, Philip. *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*. Washington, DC: U.S. Department of Homeland Security National Protection and Programs Directorate, March 23, 2011. http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

Retail Industry Leaders Association. "Strengthening Security By Heightening Awareness: New Products and Tools from the Commercial Facilities Sector-Specific Agency." *RILA Report: Asset Protection* 4, no. 2 (2010). http://www.rila.org/news/newsletters/assetprotection/May2010/Pages/StrengtheningSecuritybyHeighteningAwareness.aspx.

Relyea, Harold C. and Henry Hogue. *Department of Homeland Security Reorganization: The 2SR Initiative*, CRS Report to Congress RL33042. Washington, DC: Congressional Research Service, September 22, 2006. http://digital.library.unt.edu/ark:/67531/metacrs9942/.

Riley, Michael. "Morgan Stanley Attacked by China-Based Hackers Who Hit Google." *Bloomberg*, March 1, 2011. http://www.bloomberg.com/news/2011-02-28/morgan-stanley-network-hacked-in-same-china-based-attacks-that-hit-google.html.

Rosenbach, Eric and Aki J. Peretz. *The National Interest, Energy Security, and the Intelligence Community*. Cambridge, MA: Harvard Kennedy School of Government, Belfer Center for Science and International Affairs, July 2009. http://belfercenter.ksg.harvard.edu/files/energy-security.pdf.

Salem, Anita, Wendy Walsh, and Owen Doherty. *Industry and Public Sector Cooperation for Information Sharing: Ports of Long Beach and Los Angeles*. Monterey, CA: Maritime Information Sharing Taskforce, September 2008. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA536271.

SCADA Test Bed Program. *Current Situation: Control Systems Security*. Produced by Energetics Incorporated, Columbia, MD. Washington, DC: U.S. Department of Energy, January 21, 2011.

Science and Technology Directorate and the Office of Electricity Delivery and Energy Reliability. *Roadmap to Secure Control Systems in the Energy Sector*. Produced by Energetics Incorporated, Columbia, MD. Washington, DC: U.S. Department of Homeland Security and U.S. Department of Energy, 2006. http://www.cyber.st.dhs.gov/docs/DOE%20Roadmap%202006.pdf

Shaw, Gillian. "Government Computers Increasingly Subject to 'Sophisticated' Attacks." *Vancouver Sun*, November 10, 2010.

Shea, Dana. *Chemical Facility Security: Issues and Options for the 112th Congress*. Washington, DC: U.S. Congressional Research Service, February 17, 2011. http://www.fas.org/sgp/crs/homesec/R40695.pdf.

Shea, Dana. *Chemical Facility Security: Reauthorization, Policy Issues, and Options for Congress*. Washington, DC: U.S. Congressional Research Service, December 23, 2010. www.fas.org/sgp/crs/homesec/R40695.pdf.

"6 CFR Part 29 Procedures for Handling Critical Infrastructure Information: Final Rule." *Federal Register* 71: 170 (September 1, 2006) p. 52262 – 52277.

State, Local, Tribal, and Territorial Government Coordinating Council. *Critical Infrastructure and Key Resources (CIKR) Protection Capabilities for Fusion Centers.* Washington, DC: U.S. Department of Justice, December 2008. http://www.ncirc.gov/documents%5Cpublic%5Csupplementaries%5CCI_KR_Protection_Capabilities_Report.pdf

State of Arizona, Division of Emergency Management. *State Partnership—Arizona*. Washington, DC: Federal Emergency Management Agency, 2011. http://www.fema.gov/pdf/privatesector/arizona_ppp.pdf.

State of Maryland Governor’s Office. *Phase II Assessment: Emergency Management in the State of Maryland*. Produced by James Lee Whitt, Associates, Jackson, NJ. Annapolis, MD: State of Maryland, August 10, 2010. http://www.gohs.maryland.gov/pdfs/witt_report.pdf.

Sternstein, Aliya. “Administration Says it Will Give Industry and Academia a Heads Up on Cyber Attacks.” *NextGov.com*, January 18, 2011. http://www.nextgov.com/nextgov/ng_20110118_5841.php.

Straw, Joseph. “Fusion Centers Forge Ahead.” *Security Management*, March 7, 2011. http://www.securitymanagement.com/article/fusion-centers-forge-ahead-006223?page=0%2C0.

Theohary, Catherine A. and John Rollins. *Terrorist Use of the Internet: Information Operations in Cyberspace.* Washington, DC: Congressional Research Service, March 8, 2011. http://www.fas.org/sgp/crs/terror/R41674.pdf.

Titch, Steven. “Citgo Security Chief Describes Private Sector Antiterror Role.” *Security Squared,* September 22, 2010. http://www.securitysquared.com/2010/09/citgo-security-chief-describes-private-sectors-antiterror-role.html.

Titus*. Preventing Government Document Leaks: Titus White Paper*. Ottawa, Canada: Titus, Inc., 2010. http://www.gtra.org/index.php/component/content/article/975.

Toner, Eric S. *Creating Situational Awareness: A Systems Approach*. Pittsburgh, PA: University of Pittsburgh Medical Center, Center for Biosecurity, June 2010. http://www.upmc-biosecurity.org/website/resources/commentary/2009-06-10-create_situ_aware.pdf.

Trust for America’s Health, Robert Wood Johnson Foundation. *Ready or Not? Protecting the Public’s Health From Diseases, Disasters, and Bioterrorism*. Washington, DC: Trust for America’s Health, Robert Wood Johnson Foundation, December 2009. http://healthyamericans.org/reports/bioterror09/pdf/TFAHReadyorNot200906.pdf.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107-56 (October 26, 2001).

U.S. Department of Defense. *Protecting the Force: Lessons from Fort Hood*. Washington, DC: U.S. Department of Defense, January 2010. http://www.defense.gov/pubs/pdfs/DOD-ProtectingTheForce-Web_Security_HR_13jan10.pdf.

U.S. Department of Defense. *Quadrennial Roles and Missions Review Report*. Washington, DC: Department of Defense, January 2009. http://www.defense.gov/news/Jan2009/QRMFinalReport_v26Jan.pdf.

U.S. Department of Health and Human Services. *Biennial Implementation Plan for the National Health Security Strategy of the United States of America*, draft. Washington, DC: U.S. Department of Health and Human Services, July 19, 2010. http://www.phe.gov/Preparedness/planning/authority/nhss/comments/Documents/nhssbip-draft-100719.pdf.

U.S. Department of Health and Human Services. *National Health Security Strategy for the United States of America*. Washington, DC: U.S. Department of Health and Human Services, December 2009. http://www.phe.gov/Preparedness/planning/authority/nhss/strategy/Documents/nhss-final.pdf.

U.S. Department of Homeland Security and U.S. Department of Defense. *Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity*. Washington, DC, U.S. Department of Homeland Security and U.S. Department of

Defense, September 2010. http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

U.S. Department of Homeland Security and U.S. Department of Energy. *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*. Washington, DC: U.S. Department of Homeland Security, 2010. http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf.

U.S. Department of Homeland Security and U.S. Department of Justice. *Considerations for Fusion Center and Emergency Operations Center Coordination.* Washington, DC: U.S. Department of Homeland Security, Federal Emergency Management Agency, and U.S. Department of Justice, May 2010. http://www.fema.gov/pdf/about/divisions/npd/cpg_502_eoc-fusion_final_7_20_2010.pdf.

U.S. Department of Homeland Security and U.S. Department of Justice. *Critical Infrastructure and Key Resources (CIKR) Protection Capabilities for Fusion Centers*. Washington, DC: U.S. Department of Homeland Security and U.S. Department of Justice, December 2008.

U.S. Department of Homeland Security and U.S. Department of Justice. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era.* U.S. Department of Homeland Security and U.S. Department of Justice, August 2006. http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

U.S. Department of Homeland Security. *Banking and Finance Sector-Specific Plan*. Washington, DC: U.S. Department of Homeland Security and U.S. Department of the Treasury, 2007. http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf.

U.S. Department of Homeland Security. *Chemical Sector Security Awareness Guide: A Guide for Owners, Operators, and Chemical Supply-Chain Professionals*. Washington, DC: U.S. Department of Homeland Security, April 2010. http://www.socma.com/assets/File/socma1/PDFfiles/GR_PDF_files/DHS_Chemical_Sector_Guide_FINAL.pdf.

U.S. Department of Homeland Security. *Chemical Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*. Washington, DC: U.S. Department of Homeland Security, 2010. http://www.dhs.gov/xlibrary/assets/nipp-ssp-chemical-2010.pdf.

U.S. Department of Homeland Security. "Commercial Facilities Sector Security and Awareness." *NIPP News*, July-August 2010. http://www.fbiic.gov/public/2010/aug/NIPP%20News_July-August2010.pdf.

U.S. Department of Homeland Security. *Commercial Facilities Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*. Washington, DC: U.S. Department of Homeland Security, 2010. http://www.dhs.gov/xlibrary/assets/nipp-ssp-commercial-facilities-2010.pdf.

U.S. Department of Homeland Security. *Critical Operational Capabilities for State and Major Urban Area Fusion Centers: Gap Mitigation Strategy*. Washington, DC: U.S. Department of Homeland Security, December 2010.

U.S. Department of Homeland Security. *Department of Homeland Security Information Sharing Strategy*. Washington, DC: U.S. Department of Homeland Security, April 18, 2008. http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf.

U.S. Department of Homeland Security. False Hospital Inspectors. Washington, DC: U.S. Department of Homeland Security, 2005.

U.S. Department of Homeland Security. *National Infrastructure Protection Plan.* Washington, DC: U.S. Department of Homeland Security, 2009. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

U.S. Department of Homeland Security. "National Infrastructure Protection Plan: Energy Sector Snapshot." U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_energy.pdf.

U.S. Department of Homeland Security. *Preventing and Defending Against Cyber Attacks*. Washington, DC: U.S. Department of Homeland Security, November 2010. http://www.dhs.gov/xlibrary/assets/defending-against-cyber-attacks-september-2010.pdf.

U.S. Department of Homeland Security. *Private Sector Resources Catalog 3.0*. Washington, DC: U.S. Department of Homeland Security, July 2011. http://www.dhs.gov/xlibrary/assets/pso-private-sector-resource-catalog-3.pdf.

U.S. Department of Homeland Security. *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*. Washington, DC: U.S. Department of Homeland Security, February 2010. http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf

U.S. Department of Justice. "Fusion Centers and Intelligence Sharing." U.S. Department of Justice, http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181.

U.S. Department of Justice. *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise.* Washington, DC: U.S. Department of Justice Global Justice Information Sharing Initiative, June 2010. http://www.ncirc.gov/documents/public/supplementaries/privacy_verification.pdf.

U.S. Government Accountability Office. *Bioterrorism: Public Health Response to Anthrax Incidents of 2001*. Washington, DC: U.S. Government Accountability Office, October 2003. http://www.gao.gov/new.items/d04152.pdf.

U.S. Government Accountability Office. *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to be Consistently Addressed*, GA0-10-628. Washington, DC: U.S. Government Accountability Office, July 2010. http://www.gao.gov/new.items/d10628.pdf.

U.S. Government Accountability Office. *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-4-780. Washington, DC: U.S. Government Accountability Office, July 2004. http://www.gao.gov/new.items/d04780.pdf.

U.S. Government Accountability Office. *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems*, GAO-11-463T. Washington, DC: U.S. Government Accountability Office, March 16, 2011. http://www.gao.gov/new.items/d11463t.pdf.

U.S. Government Accountability Office. *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO-10-338. Washington, DC: U.S. Government Accountability Office, March 2010. http://www.gao.gov/new.items/d10338.pdf.

U.S. Government Accountability Office. *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*, GAO-11-117. Washington, DC: U.S. Government Accountability Office, January 12, 2011. http://www.gao.gov/new.items/d11117.pdf.

U.S. Government Accountability Office. *Influenza Pandemic: Lessons from the H1N1 Pandemic Should Be Incorporated into Future Planning*. Washington, DC: U.S. Government Accountability Office, June 2011. http://www.gao.gov/new.items/d11632.pdf.

U.S. Government Accountability Office. *Information Security: Concerted Response Needed to Resolve Persistent Weakness*, GAO-10-536T. Washington, DC: U.S. Government Accountability Office, March 2010. http://www.gao.gov/new.items/d10536t.pdf.

U.S. Government Accountability Office. *Information Sharing: DHS Could Better Define How It Plans to Meet Its State and Local Mission and Improve Performance Accountability*, GAO-11-223. Washington, DC: U.S. Government Accountability Office, December 2010. http://www.gao.gov/new.items/d11223.pdf.

U.S. Government Accountability Office. *Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investments*, GAO-11-455. Washington, DC: U.S. Government Accountability Office, July 2011, http://www.gao.gov/new.items/d11455.pdf.

U.S. Government Accountability Office. *Information Sharing: Federal Agencies are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results*, GAO-10-972. Washington, DC: U.S. Government Accountability Office, September 2010. http://www.gao.gov/new.items/d10972.pdf.

U.S. Government Accountability Office. *Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes*, GAO-10-867. Washington, DC: U.S. Government Accountability Office, August 2010. http://www.gao.gov/new.items/d10867.pdf.

U.S. Homeland Security Council. *National Strategy for Homeland Security*. Washington, DC: U.S. Homeland Security Council, October 2007. http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf.

U.S. Office of the National Counterintelligence Executive. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY 2008*. Washington, DC: U.S. Office of the National Counterintelligence Executive, July 23, 2009. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA506093&Location=U2&doc=GetTRDoc.pdf.

U.S. Office of the National Counterintelligence Executive. *The National Counterintelligence Strategy of the United States of America*, NCIX-2010-002. Washington, DC: U.S. Office of the National Counterintelligence Executive, 2009. http://www.ncix.gov/publications/policy/NatlCIStrategy2009.pdf.

U.S. Transportation Security Administration. "Pipeline Security: Transportation Sector Network Management." U.S. Transportation Security Administration. http://www.tsa.gov/what_we_do/tsnm/pipeline.shtm.

Van Cleave, Michelle K. *Counterintelligence and National Strategy*. Washington, DC: National Defense University Press, April 2007. http://www.ndu.edu/CISA/docUploaded/Web%20version%20Van%20Cleave.pdf.

Wade, Cheryl. *The California Law Enforcement Community's Intelligence-Led Policing Capacity*. Monterrey, CA: Naval Postgraduate School, December 2010.

Weiss, Eric N. *Banking and Financial Infrastructure Continuity: Pandemic Flu, Terrorism, and Other Challenges*. Washington, DC: U.S Congressional Research Service, May 4, 2009. http://www.fas.org/sgp/crs/misc/RL31873.pdf.

Weitz, Dr. Richard. "DHS Grapples with Cyber Threats." *Second Line of Defense*, April 27, 2011. http://www.sldinfo.com/?p=17707.

West Virginia Intelligence Fusion Center. *West Virginia Intelligence Fusion Center Privacy Policy*. Charleston, WV: West Virginia Intelligence Fusion Center, February 25, 2011. http://www.wv.gov/fusioncenter/Documents/West%20Virginia%20WVIFC%202-25-2011.pdf.

Whitehead, Steve. "Corporate Counterintelligence—Protecting Business Information." *Computer Business Review*, June 2003. http://cbr.co.za/regular.aspx?pklRegularId=1390.

White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: White House, May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

White House. *National Security Strategy*. Washington, DC: White House, May 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

White House. *National Strategy for Counterterrorism*. Washington, DC: White House, June 2011. http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf.

White House. *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*. Washington, DC: White House, October 2007. http://www.fas.org/sgp/library/infoshare.pdf.

White House*. The Comprehensive National Cybersecurity Initiative*. Washington, DC: White House, March 2, 2010. http://www.fas.org/irp/eprint/cnci.pdf.

White House. *The National Strategy to Secure Cyberspace*. Washington, DC: White House, February 2003. http://georgewbush-whitehouse.archives.gov/pcipb/.

VeriSign Intelligence Operations Team. *Distributed Denial of Service (DDOS) Attacks: An Overview and Analysis.* Mountain View, CA: VeriSign, Inc., June 4, 2010. http://www.fsisac.com/files/public/db/p244.pdf.

Verizon RISK Team. *2011 Data Breach Investigations Report*. New York: Verizon, 2011 http://www.secretservice.gov/Verizon_Data_Breach_2011.pdf.

Zakaria, Tabassum. "US Security Agency Opens to Outsiders on Cyber Safety." Reuters, September 20, 2011. http://www.reuters.com/article/2011/09/20/usa-cyber-nsa-idUSS1E78J19N20110920.