NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

PUBLIC-PRIVATE SECTOR INTELLIGENCE COORDINATION

FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL

July 11, 2006

JOHN T. CHAMBERS
WORKING GROUP CO-CHAIR
PRESIDENT AND CHIEF EXECUTIVE OFFICER
CISCO SYSTEMS, INC.

CHIEF GILBERT G. GALLEGOS
WORKING GROUP CO-CHAIR
CHIEF OF POLICE (RET.)
ALBUQUERQUE, NEW MEXICO POLICE DEPARTMENT

Acknowledgements

Working Group Members:
John T. Chambers, President and CEO, Cisco Systems, Inc., NIAC Vice Chairman
Gilbert G. Gallegos, retired Chief of Police, City of Albuquerque, New Mexico
Erle A. Nye, Chairman Emeritus, TXU Corp., NIAC Chairman
Alfred R. Berkeley III, Chairman and CEO, Pipeline Financial Group, and former President and Vice Chairman of NASDAQ
Craig R. Barrett, Chairman of the Board, Intel Corp.
Chief Rebecca F. Denlinger, Chief, Cobb County (Georgia) Fire & Emergency Services
Commissioner Raymond W. Kelly, Police Commissioner, City of New York
Thomas E. Noonan, Chairman, President and CEO, Internet Security Systems, Inc.
Gregory A. Peters, Former President and CEO, Internap Network Services Corp.
Bruce Rohde, Chairman and CEO Emeritus, ConAgra Foods, Inc.

Study Group Members:

Public/Private Sector
Kenneth Watson, Cisco Systems, Inc.
David Frigeri, Internap Network Services Corp.
William Muston, TXU Corp.
Bill Aimetti, Depository Trust and Clearing Corp.
Clay Detlefsen, International Dairy Foods Association
Dan Bart, Telecommunications Industry Associations
Diane VanDe Hei, Association of Metropolitan Water Agencies
Lou Leffler, North American Electric Reliability Council
Nancy Wilson, Association of American Railroads
Robin Roberts, Cisco Systems, Inc.
Alfred Hancock, Xcel Energy
Steve Carey, Depository Trust and Clearing Corp.
Brian Willis, Intel Corp.
Darren Lacey, Johns Hopkins University Hospital

Government
Clint Hubbard, Police Department, City of Albuquerque, New Mexico
Vic Erevia, Secret Service
Lt. Paul Mauro, New York City Police Department (NYPD)
Paul Bennett, New York City Department of Environment (DEP)
Stuart Shannonhouse, Cobb County, Georgia
Tom Donahue, Central Intelligence Agency
Margie Gilbert, Central Intelligence Agency
Warren “Jack” Russell, Department of Defense
G. Rick Wilson, National Security Agency
Monica Gaughan, National Geospatial-Intelligence Agency
Gail Seavey, Federal Bureau of Investigation

Gary Loeffert, Federal Bureau of Investigation
Dean Carver, Office of the Director of National Intelligence
Scott Harper, Office of the Director of National Intelligence
Arnold Abraham, Office of the Director of National Intelligence

DHS Resources
Infrastructure Partnerships Division
R. James Caverly
Nancy J. Wong
Jenny Menna
Gail Kaufman, SRA contractor
Michael Schelble, SRA contractor
John MacGaffin, consultant to General Dynamics
John Tritak, Good Harbor Consulting
Office of Intelligence and Analysis
James (Tommy) Faust
Melissa Smislova
Robert Beecher
Bob Whitaker
Donnie Young

Table of Contents

Executive Summary

Charter

In July 2004, President Bush asked the NIAC to study whether the Federal Government and its private sector partners could improve the way the Intelligence Community (IC) coordinates with critical infrastructure owners and operators. In response, the NIAC created the Intelligence Coordination Working Group. Based on the Working Group's inputs, this is the Council's report.

Goal

The Working Group focused principally on the way information flows between the IC and the private sector. Below are the two questions that governed the Working Group's approach throughout the process:

1. In what ways can the IC help critical infrastructure owners and operators?
2. In what ways can critical infrastructure owners and operators help the IC?

Approach

The Working Group created a Study Group of more than 30 representative experts from the private sector and the IC to provide input to the Working Group to assist the Council in its formulation of findings and recommendations. The Study Group received briefings about existing information sharing mechanisms within the government, and also convened four day-long workshops where experts articulated information requirement shortfalls, discussed ways to refine current information sharing mechanisms, and shared lessons learned from recent incidents. The Working Group also interviewed Chief Executive Officers (CEOs) from selected Critical Infrastructure Sectors. Appendix A provides a summary of the views of the CEOs. Based on these combined inputs, the Council developed nine findings and eight recommendations. The Study Group conducted case studies on four recent terrorist- or threat-related events to illuminate the findings it presented to the Working Group. Appendix B includes a summary of the case studies.

Scope

The Council did not seek to repeat the efforts of numerous previous and contemporaneous studies on information sharing and intelligence coordination. Instead, the group leveraged the results of these existing studies and added two unique perspectives to the subject—the CEO perspective and the comprehensive involvement of critical infrastructure owners and operators as well as intelligence agencies. This report is significant in that it mirrored the efforts of the Homeland Security Advisory Council. Meeting during the same period, both groups, independent of each other, reached nearly identical conclusions and developed similar recommendations despite involving different stakeholders in their processes. These complementary conclusions strongly validate the efforts of both groups, and add significant weight to both sets of recommendations. Appendix C in this document provides a review of the current structure, mission, and authorities pertaining to the IC within the United States. Appendix D describes the critical infrastructure owner/operator environment, governance, and relationships.

Impact of Recent Changes

Changes in governance and structure in both the IC and the critical infrastructures have taken place since the President commissioned this report. The two most significant changes are the establishment of the Office of the Director of National Intelligence (ODNI) and the creation of the Critical Infrastructure Partnership Advisory Council (CIPAC). These new organizations provide a framework providing single primary points of contact for both the government and the private sector, which was a requirement repeated often by Study Group participants and echoed in the other studies reviewed by the Council. This report's recommendations provide additional details regarding actions that ODNI and CIPAC, as well as the Department of Homeland Security (DHS), will need to implement as all these organizations continue to develop.

In December 2005, the President issued guidance regarding the Information Sharing Environment (ISE), created by Executive Order 13388 and housed within ODNI. This guidance addresses several of the Council's recommendations. Specific guidance to heads of Executive departments and agencies charged them to:

- Leverage ongoing information sharing efforts in the development of the ISE;
- Define common standards for how information is acquired, accessed, shared, and used within the ISE;
- Develop a common framework for the sharing of information between and among Executive departments and agencies and State, local, and tribal governments, law enforcement agencies, and the private sector;
- Standardize procedures for sensitive but unclassified information;
- Facilitate information sharing between Executive departments and agencies and foreign partners;
- Protect the information privacy rights and other legal rights of Americans; and
- Promote a culture of information sharing.[1]

Findings

The Working Group interviewed chief executives from a cross-section of the critical infrastructure industries to discuss their views on improving information sharing between the private sector and IC. These interviews examined the issues of information sharing within the broader context of a CEO's role in managing business and operational risks in the aftermath of September 11. Following 9/11, nearly all CEOs examined the ways in which they managed strategic risk, focusing especially on the adequacy of their existing security measures and the gaps in coverage.

Finding 1: In today's environment, personal relationships are integral to successful information sharing between the private sector and the government. Conversations among people who already know and trust each other are more fruitful than conversations among those that do not.

[1] George W. Bush, "Guidelines and Requirements in support of the Information Sharing Environment," Memorandum for the Heads of Executive Departments and Agencies, December 16, 2005

Finding 2: Given the high turnover rate for public and private sector personnel, both sides should minimize their dependence on personal relationships while institutionalizing the trust between the public and private sectors.

Finding 3: A lack of critical infrastructure subject-matter expertise can seriously hamper the process for analyzing intelligence.

Finding 4: The government's intelligence dissemination processes do not deliver the necessary information consistently to the right people in the private sector in sufficient time to act.

Finding 5: Private sector information-sharing mechanisms and processes vary widely in capabilities, maturity, and reach.

Finding 6: Despite the implementation of the Protected Critical Infrastructure Information (PCII) program, many in the private sector continue to have a concern about information protection. The private sector also worries about the fact that no one person or group has yet challenged PCII and that no court has upheld it.

Finding 7: At present, there is no threat-information clearinghouse for critical infrastructure owners and operators to use to make sound business decisions.

Finding 8: Critical infrastructure sectors lack an established and common process to provide information to and receive information and intelligence from the IC.

Finding 9: The proliferation of "Sensitive But Unclassified" (SBU) caveats attached to otherwise unrestricted (unclassified) government documents inhibits information sharing and confuses recipients.

Recommendations

If all relevant public and private sector parties adopt the recommendations outlined below, the Council believes the United States will have significantly strengthened the protection of its most critical infrastructures.

Recommendation 1: **Senior Executive Information Sharing**
Develop a voluntary executive-level information sharing process between critical infrastructure CEOs and senior intelligence officers. Begin with a pilot program of volunteer chief executives of one sector, with the goal of expanding to all sectors.

Recommendation 2: Best Practices for the Private Sector
The U.S. Attorney General should publish a best practices guide for private sector employers to avoid being in conflict with the law. This guide should clarify legal issues surrounding the apparent conflict between privacy laws and counter terrorism laws involving employees. Moreover, it should clarify the limits of private sector cooperation with the IC.

Recommendation 3: Existing Mechanisms
Leverage existing information-sharing mechanisms as clearinghouses for information to and from critical infrastructure owners and operators. This takes advantage of the realities that exist sector by sector.

Recommendation 4: National-Level Fusion Capability
Establish or modify existing government entities to enable national- and state-level intelligence and information fusion capability focused on Critical Infrastructure Protection (CIP).

Recommendation 5: Staffing
Create additional "Sector Specialist" positions at the executive and operational levels as applicable in the IC. These specialists should be civil servants who have the ability to develop a deep understanding of their private sector partners.

Recommendation 6: Training
Develop an ongoing training and career development program for sector specialists within intelligence agencies.

Recommendation 7: RFI Process
Develop a formal, and objectively manageable, homeland security intelligence and information requirements process, including requests for information (RFIs). This should include specific, bi-directional processes tailored sector by sector.

Recommendation 8: Standardize SBU Markings and Restrictions
The Federal government should rationalize and standardize the use of SBU markings, especially "For Official Use Only" (FOUO), and publish standard handling instructions clearly for all intended recipients.

1. Introduction

A. Charter

President George W. Bush asked the NIAC in July 2004 to study whether the Federal Government and its private sector partners could make improvements in "the utilization and effectiveness of intelligence capabilities to protect critical infrastructure by improving interactions and information requirements definition between the Intelligence Community (IC) and critical infrastructure sectors." In response to the President's request, the NIAC created a Working Group to explore ways to improve interaction between the IC and critical infrastructure owners and operators.

B. Goal

The Working Group's principal focus was exploring the way in which information flows between the IC and the private sector from a strategic, CEO perspective, and at the operational, incident management level.

The Working Group kept two questions at the forefront of its efforts:

- In what ways can the IC help critical infrastructure owners and operators?
- In what ways can critical infrastructure owners and operators help the IC?

C. Approach

The Working Group created a Study Group of more than 30 representative experts from the private sector and the IC to provide input to the Working Group and help the Council formulate findings and recommendations. The Study Group held regular meetings in which they received briefings about existing information sharing mechanisms within the government, particularly within DHS. The Study Group also convened four day-long workshops where experts articulated information requirement shortfalls, discussed ways to refine current information sharing mechanisms, and shared lessons learned from recent incidents: the Northeast Blackout of August 2003, the Financial Target Threat of August 2004, the London Subway Bombing of July 2005, and the New York City Subway Threat of October 2005. Appendix B contains detailed findings and conclusions from the case studies. The Working Group also interviewed Chief Executive Officers from across the Critical Infrastructures/Key Resources (CI/KR). Appendix A contains a summary of their views.

D. Scope

There have been multiple recent studies covering various aspects of information sharing, intelligence reform, public-private cooperation to combat terrorism, and other topics related to this task. The Council found itself in significant agreement with these reports, but its work brings two significant additional perspectives missing from previous studies.

The four workshops, which included study group members, represented for the first time leaders from each of the critical infrastructure sectors to discuss issues in the same room with senior

representatives from many of the nation's key intelligence agencies. Indeed, some of the IC representatives stated that even they had not all come together in one room before. Therefore, one unique perspective of this report is the involvement of a broad intersection from the critical infrastructures and the IC.

The second unique aspect of this study is the CEO perspective. Chief executives bring both an urgent practicality and a strategic outlook to problem solving. It was eye-opening for some workshop participants to see the unique needs for information at *both* the strategic executive level and the operational incident management level.

2. Information Sharing

Information sharing is vital for protecting the nation's CI/KR, yet views and definitions of this function vary widely. Since DHS' inception, strategies for infrastructure protection have evolved and the aims and scope of information sharing have expanded. For the purposes of this study, information sharing pertains to information flowing between the IC and critical infrastructure owners and operators. Appendix C is a detailed description of the IC, and Appendix D describes critical infrastructure definitions, governance, and organization. Appendix E is an in-depth discussion of information sharing as it applies to critical infrastructures and the IC.

DHS has begun implementation of a number of mechanisms in an effort to improve information sharing with critical infrastructure owners and operators. These include:

- Homeland Security Information Network (HSIN)
- Executive Notification System (ENS)
- Critical Infrastructure Partnership Advisory Council (CIPAC)
- Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)
- National Infrastructure Coordinating Center (NICC)
- Protected Critical Infrastructure Information (PCII)

Members of the Council received presentations on each of these programs, and noted that they represent positive, but incremental progress. Nonetheless, the entire Council found a number of areas where intelligence coordination still needs improvement.

A. Definition Ambiguity

The term "information sharing" is so overused that its meaning must be redefined for nearly every instance that it is used. Web searches for "information sharing" return over 500 million links, and narrowing the search to "homeland security information sharing" still nets more than 16 million hits. For example, the entire concept of Information Sharing and Analysis Centers (ISACs) is encouraged under Presidential Decision Directive 63 (PDD 63). Moreover, ISACs are designed for sharing information on threats, vulnerabilities, countermeasures, and best practices within and across critical infrastructure sectors. The new Information Sharing Environment (ISE) program within ODNI focuses on linking resources of Federal, state, local, tribal entities and the private sector to share relevant information on terrorism.

This study focused on enhancing the sharing of risk information to critical infrastructure partners, especially between owners and operators and the IC. This involves a wide variety of participants, including law enforcement, CEOs, corporate security officers, sector-specific associations, and IC analysts. The study's focus also extends from proactive risk management and long-term, strategic planning to reactive, pre-incident, near-term deterrence and protection, and to post-incident response and recovery.

The information shared between the private sector and the IC falls into three primary categories: (1) strategic threat information that drives investment and expenditures; (2) situational awareness information around assets and systems on a daily basis, including notification that nothing is threatening; and (3) alerts and warnings of a potential imminent threat.

B. Previous Studies

The Council learned from several relevant studies of information sharing, the IC, intelligence reform, and CIP. Primary references include:

- Evaluation and Enhancement of Information Sharing and Analysis**,** NIAC, July 13, 2004
- The 9/11 Commission Report, July 22, 2004
- Intelligence and Information Sharing Initiative Final Report and Recommendations, Homeland Security Advisory Council, December 2004
- The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction Report, March 31, 2005
- Homeland Security Intelligence and Information Fusion, Homeland Security Advisory Council (HSAC), April 28, 2005
- Homeland Security Information Sharing between Government and the Private Sector Final Report, HSAC, August 10, 2005
- Lessons Learned Information Sharing Initiative: Homeland Security Intelligence Requirements Process, HSAC, December 2005

It is important to note that both the NIAC and the HSAC studied aspects of information sharing and intelligence coordination at the same time, but with different groups of stakeholders. The fact that both studies came to very similar conclusions, and are making similar recommendations, strongly validates both efforts.

It is also important to note that DHS and ODNI have implemented several of the recommendations from these previous studies. Even though they and others have made progress, there is more that needs to be done. This purpose of this report's recommendations is to illuminate the needs that other studies have not highlighted and to accelerate the progress that has already been made.

3. Findings

The Council arranged its findings into five broad categories: trust, analysis, dissemination, information protection, and other supporting processes. It is impossible to consider any one category in isolation—issues in one category affect all the others. For example, failure to protect information adequately can significantly affect trust, and process flaws can skew analysis, leading to wrong conclusions. The Council offers these categories as an aid to understanding.

A. Trust

Finding 1: In today's environment, personal relationships are integral to successful information sharing between the private sector and the government. Conversations among people who already know and trust each other are more fruitful than conversations among those who do not know and trust each other.

The Council identified several barriers to trust between the IC and critical infrastructures, including:

- Wide variability of expertise and experience among government "sector specialists";
- Multiple, often duplicative, requests for information from too many distinct government entities;
- Release of private sector information by government to unintended or inappropriate audiences;
- Government regulation or the threat of new regulation;
- The lack of a common glossary of terms; and
- A deficiency in cross-organizational understanding.

Critical infrastructure owners and operators do not believe the government has the necessary expertise to understand the information they provide, and therefore fear it may be misused or that it may inform misguided policies. Owners and operators also complain that the government only informs them about new CIP-related policies and procedures that affect them after the government has are already completed them without private-sector input.

Finding 2: There was also a strong sentiment that because of personnel turnover throughout the public and private sectors, the Federal Government must institutionalize mechanisms that foster trust, thereby minimizing the dependence on personal relationships. While personal relationships are important, especially at the executive level, these must be secondary to established and commonly understood processes, which would serve to institutionalize trust relationships.

An example of institutionalized trust is the U.S. government's classified material management program. The government identifies and establishes positions (called "billets") with carefully defined "need to know" parameters. Via background checks, the government vets all individuals seeking security clearances and the government then assigns those positions before officials

grant access to classified material. Similarly, facilities for transmission and storage of classified information are built, inspected, and certified to government-defined specifications. A cleared employee in a cleared facility receiving information either by secure telephone, video, or in person, knows he or she can trust the other person, even though they may have never met. Defined billets carry an assumption of trust based on process.

B. Analysis

Finding 3: A lack of critical infrastructure subject-matter expertise can seriously hamper the process of analyzing intelligence. The challenge is how to increase that level of understanding without crossing the line between the role of government and the role of business.

Accurate analysis of threat information requires private sector input, and the IC participants agreed with this finding. Participants discussed numerous cases. For example, government analysts believed stolen derail devices represented a significant threat, but railroad sector experts were aware of long-standing mitigating measures that rendered this risk inconsequential.

The Federal government needs sector-specific critical infrastructure expertise to help fuse all-source data to produce accurate and timely threat information and intelligence products. Something that might seem like benign information to an intelligence analyst might actually be an essential piece of the puzzle only understood by a private -sector expert. Having the private sector's insight earlier in the intelligence process might help put some matters into perspective before the government spends scarce time and resources on issues that might not be relevant. Even worse, government analysts could miss a critical indicator and fail to understand its threat implications.

> *"The Intelligence Community…needs to think more creatively and, above all, more strategically about how it taps into external sources of knowledge. This may include recognizing that the Community may simply not be the natural home for real expertise on certain topics. While economics analysts, for example, can and do play a valuable role in the Community, economists at the Federal Reserve, World Bank or private sector companies investing millions in emerging markets are likely to have a better handle on current market conditions. Relying on these experts might free up Community resources to work more intensely on finding answers no one else has."*[2]

Designating private sector subject matter experts (SMEs) to work with intelligence analysts would reduce the IC's need to poll an entire sector for details and factors impacting the information they were analyzing. In addition to helping analysts understand the impact of threat information, these subject-matter experts could also keep the IC updated on the implications of constantly changing technology in the private sector.

[2] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction – Report to the President of the United States, March 31, 2005.

Along with the benefits of sharing private-sector subject-matter expertise with the IC come challenges. Some sector representatives would prefer to collocate their experts with intelligence analysts, in government operations centers, to help sort through unrefined information to assist the IC in prioritizing its analysis. Other private sector representatives, especially those associated with multinational corporations or multinational contracts, would prefer that the government train analysts, consult with subject matter experts (SMEs), or hire consultants. In all cases, there must be a clear line between the functions of intelligence and business. It is not the private sector's business to collect or analyze intelligence, nor is it the government's business to help the private sector make a profit.

Besides functional differences, there are also cultural differences between the private sector and the IC. Traditionally, the IC is driven by the requirement to determine the intent and capabilities of elements that could threaten national security. This has resulted in development of various sources and methods, and the subsequent need to protect them with stringent rules limiting sensitive information to those with a strictly defined "need to know." The keeping of secrets is integral to the operations of the IC.

Industry, however, has learned that speed translates to wins in the marketplace and greater profits. Companies have built extensive marketing and communications capabilities to share marketing information broadly with customers, partners, and the public. Advancements in information technology continue to accelerate that information flow. The trend is toward more and more interactive transactions, with suppliers and customers sharing increasing amounts of information. Automated ordering and delivery depends on some level of knowledge of transaction information, such as address, phone number, payment information, product or service details, and other customer requirements. Increasing the speed and accuracy of transactions is integral to most private sector operations.

The Council considered several options to address these subject matter expertise and cross-cultural challenges. One alternative is for the IC to hire critical infrastructure sector-specific SMEs or contract with them as consultants. If the government hires these SMEs as government employees, there would be a challenge keeping their knowledge current. Given the nature of their business, consultants may be able to remain more current than are government employees. A benefit to this alternative is that it preserves a clear boundary between the private sector and IC in terms of liability, authorities, and mission.

Another option is for the IC to train their employees in order to develop sufficient critical infrastructure sector-specific subject matter expertise. There are several challenges to overcome with this option, including the considerable time needed to develop suitable expertise and, again, keeping subject-matter experts' knowledge current. This option also has the benefit of preserving a clear boundary between the private sector and IC in terms of liability, authorities, and mission.

A third approach is for the IC to augment their analytic process with private sector experts. This could be in the form of short-term interactions on an as-needed basis. A challenge with this alternative is that the IC needs to know what to ask for, and recognize that a knowledge gap exists. Longer-term placements within the IC may be preferable, but the challenge is identifying the correct expertise and finding appropriate individuals with the ability to reach back into their

sectors in a timely manner. This approach has several benefits. It provides the opportunity to develop trusted relationships among key individuals and groups across the private sector and the IC. It also provides the opportunity to improve requirements for IC-private sector interaction by sharing operational, vocabulary, and cultural understanding.

All three options should be available so that individual sectors and companies can make choices appropriate to their working environment, legal, and business considerations.

Related to this finding, the Council explored the idea of government analysts helping the private sector with threat and risk assessments. Some private sector participants expressed a desire to use raw intelligence data for operational-level situational awareness, unfiltered by government analysis. However, others disagreed. Some critical infrastructure sectors (e.g., the Railroad and Water Sectors) have a strong sector-level threat and risk analysis capability. Additionally, various large corporations have developed a similar capability tailored to their business needs. The consensus among Working Group participants was that the private sector does not have a strong demand for intelligence analysis expertise for assisting with business threat or risk analysis.

C. Dissemination

Finding 4: The government's intelligence dissemination processes do not deliver the necessary information consistently to the right people in the private sector in sufficient time to act.

One of the case studies conducted by the Study Group was the threat advisory to Financial Sector targets in August 2004. Officials based the alert on information in documents seized from terrorists that mentioned specific companies. In gaining permission to release from original classification authorities, government personnel decided to inform only companies specifically mentioned in the documents, plus NYPD. Government officials asked the companies invited to the briefing not to tell others because of the sensitivity of the information. By the time initial briefings occurred, the press was already carrying banner headlines with substantive details, obviating government attempts at limited disclosure.

On the one hand, some financial services companies that the government had not briefed actually had offices in the buildings threatened. On the other hand, some companies named in the documents were not, in fact, associated with the buildings. In the case of Citicorp, another company owned and managed the "Citicorp" building and several other companies occupied it. There were no Citicorp employees concurrently associated with the building.

Financial sector representatives also stated that a threat against one or two major companies affects the entire sector because their sector is so tightly integrated.

Beyond the financial services sector, at least one telecommunications company shared a wall with one of the target financial services buildings, but since the intelligence information did not identify telecommunications companies as targets, officials did not notify them. In addition,

transportation and electric power facilities traversed around and under the targeted buildings, but again officials did not notify representatives from the affected companies.

Finding 5: Private sector information sharing mechanisms and processes vary widely in capabilities, maturity, and reach.

The IC must understand these differences as it determines with whom to share information.
The ISACs operate under a variety of business models: some collect membership dues, some receive government funding or employ government resources in kind, and some use third-party vendors to manage operations. Some sectors have chosen not to implement ISACs.

Some ISACs serve close to 100 percent of constituent firms within their sectors, while others serve less than 20 percent of firms. Some ISACs have personnel with security clearances who can receive classified data while others work entirely with sensitive but unclassified data. Some maintain 24/7 watch desks and analysis capabilities and others do not. Most ISACs focus on managing incident data (principally disseminating government alerts and warnings to members), but some have leveraged their networks to collect and share additional information, such as best practices and industry security guidelines. Some ISACs focus primarily on cyber incidents, while others focus primarily on physical incidents. The Council found that the government should not assume that in all sectors it should communicate the threat solely to an ISAC. Sector Coordinating Councils (SCCs) and their counterpart Government Coordinating Councils (GCCs) can assist DHS and other government agencies regarding with which organizations to coordinate threat and other intelligence information.

D. Information protection

Finding 6: Despite the implementation of the Protected Critical Infrastructure Information (PCII) program, many in the private sector continue to have a concern about information protection. The private sector is also concerned that PCII has not been legally challenged and upheld. Several of the participants suggested the government implement a new information classification mechanism for CIP.

Government and private sector representatives agree they want information protection mechanisms that shield them from the harmful consequences of release to unintended audiences or for unintended purposes. The success of the initiatives and mechanisms created to improve information and intelligence sharing among the government and private Sector entities hinges on the success of protection policies like PCII.

The PCII program is relatively new. Lessons learned from the PCII program illuminate some of the shortfalls of existing policies and laws. The Critical Infrastructure Information Act of 2002 shields private sector from Freedom of Information Act (FOIA) disclosure of Critical Infrastructure Information, but the law lacks the assurance that comes from being challenged and successfully defended in court. The program also lacks tracking and accountability mechanisms for guaranteeing protection from disclosure. Without mechanisms put in place to address these concerns, private sector infrastructure operators will remain reluctant to share information with the government.

The IC uses the *Originator Control* "ORCON" handling caveat to limit dissemination, but no such corollary exists for unclassified information. Establishment of originator control rules for sensitive but unclassified information might improve organizational trust and speed information handling. The PCII program has proposed similar mechanisms—*submitter consent* and *limited dissemination*—to be incorporated into its final rules for sharing information. Under these rules, when an entity submits information, it can both limit the organizations that receive the information and it can add additional organizations that have not met the requirements for participation in the program. If implemented, these rules would also help address private sector concerns that submitting their sensitive critical infrastructure information would effectively cede all control of their business interests.

E. Process

Finding 7: At present, there is no threat-information clearinghouse for critical infrastructure owners and operators to use to make sound business decisions. These owners and operators are continuing to be bombarded by multiple, uncoordinated, duplicative requests and advisories from multiple government offices at multiple levels. Many government departments and agencies are involved in critical infrastructure protection, have specialized critical infrastructure protection offices, and request related information from, and provide alerts and advisories to, the private sector. Private sector decision makers are often confused regarding which government agency to turn for coordinating critical infrastructure protection. Some sector organizations have existing relationships, which they will continue to maintain and grow. However, most critical infrastructure stakeholders do not know where to go to get their questions about threats answered or to report threat information.

The Federal Government has already designated existing SCCs, and ISACs, as appropriate, to represent ready-made vehicles for sector-specific information and intelligence fusion.

Finding 8: Critical infrastructure sectors lack an established and common process to provide information to and receive information and intelligence from the IC.

Some private sector Study Group participants said that they would benefit from a formalized immediate "ready contact" to whom to report information or circumstances that appear unusual or suspicious. An example of one successful such ready contact is the New York City Police Department's Operation NEXUS program. NEXUS provides an alerting mechanism, with examples of activity related to specific industries that may be of possible concern to law enforcement.

An existing RFI process has existed for some time in the IC for internal use, but it was not designed for private-sector use. The needed public-private RFI process would allow the private sector to identify specific information requirements and obtain background threat context for risk analysis and assessments and to support protection decisions. Private sector decision makers would use the information to develop a business case for enhanced protection that will drive the protective capabilities of a site or company. Such an RFI process would require central coordination for improved accountability and necessary breadth of information.

In addition to threat information, the private sector would benefit from initial guidance from the government on suggested actions to take. The Council learned from several private sector security experts who provided numerous examples where threat or incident reports left decision makers wondering what specific actions they should take. For example, after the London subway bombings, companies wanted to know whether the government would recommend they call their employees back from London. The private sector representatives pointed out that their companies have Continuity of Operations plans for their specific companies and industry sectors for which they rely on government threat and risk information.

Again, the New York City Police Department Operation NEXUS program provided a positive example. In addition to giving examples of sector specific threat indicators ("what to look for"), it also provides recommended threat response plans, similar to Department of Defense (DoD) Operations Plans.

Finding 9: The proliferation of SBU caveats attached to otherwise unrestricted (unclassified) government documents inhibits information sharing and confuses recipients. According to a Government Accountability Office (GAO) report in March 2006: "Federal agencies report 56 different sensitive but unclassified (SBU) designations (16 of which belong to one agency) to protect sensitive information – from law or drug enforcement to controlled nuclear information.

> *"For most designations there are no government-wide policies or procedures that describe the basis on which an agency should assign a given designation and ensure that it will be used consistently from one agency to another. Without such policies, each agency determines what designations and associated policies to apply to the sensitive information it develops or shares. More than half the agencies reported challenges in sharing such information. Finally, most of the agencies GAO reviewed have no policies for determining who and how many employees should have authority to make sensitive but unclassified designations, providing them training on how to make these designations, or performing periodic reviews to determine how well their practices are working."* [3]

Different agencies within the Federal Government define FOUO differently, resulting in a variety of handling restrictions. One common marking prohibits dissemination of FOUO-marked information to foreign nationals. In some cases, foreign nationals in decision-making positions could utilize this information to make better-informed decisions.

There are other issues related to the FOUO marking. First, some in the private sector were dismayed that information they provided to the government came back to them with the FOUO labeling, specifically restricting further dissemination. This causes confusion at best, and distrust at worst. Some of the private sector participants noted another apparent misuse of the marking at times, seeing openly reported information repeated in a government document and labeled

[3] "Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information," GAO-06-385, March 2006

FOUO. This haphazard approach to FOUO is counterproductive to the effective sharing of information to protect critical infrastructures.

Although not used with unclassified government documents, "Originator Control" (ORCON) is also of concern. ORCON is a caveat commonly used by the IC to ensure originators can control dissemination of products for which they are responsible. Other intelligence agencies or government offices may not alter, downgrade, or excerpt from an ORCON-stamped document without express permission of the originator.

The discussion of the ORCON caveat surfaced during the work on case studies of recent incidents. The result of ORCON on private sector owners and operators was conflicting information from government agencies, or lack of DHS comment on threat information received from governmental parties other than DHS. This led to some confusion in the private sector, and added to misunderstanding and distrust of government. More importantly, it slowed down the vital dissemination of threat information.

In the case of the 2005 NYC Subway Threat, the private sector requested additional information from DHS. However, DHS personnel could not obtain the necessary permissions from the originators of the information it had, so they could not comment. Private sector representatives said that this silence from DHS added to the confusion and anxiety surrounding this incident.

4. Recommendations

Each of the following recommendations by the Council addresses issues that cross multiple categories of findings. Together, they focus on actions the President can take to improve five key aspects of public/private-sector intelligence coordination:

- Trust between the IC and critical infrastructure owners and operators;
- The quality and timeliness of intelligence analysis;
- Dissemination to the right decision makers in a timely manner;
- Protection of sensitive government and private sector information; and
- Administrative processes required for effective public-private coordination.

A. Recommendation 1: Senior Executive Information Sharing Mechanism

Develop a voluntary executive-level information sharing mechanism between critical infrastructure CEOs and senior intelligence officers. DHS should expand the CIPAC or the National Infrastructure Coordinating Center (NICC) to include a voluntary executive-level forum for critical infrastructure CEOs and intelligence executives. Begin with a pilot program of voluntary chief executives of one sector, with the goal of expanding to all sectors.

For the pilot program, a small, high-level government team should meet with CEOs in the selected sector. The objective would be to determine what kind of knowledge is needed and how trust can be created to have an effective information sharing program with two dimensions: first at the level of CEO to IC Senior Management; second, at the level of private sector expert to government expert within the sector.

There are already many efforts to share information and many of them work well. Adding CEOs to the process is the focus of this recommendation. Currently, interactions with CEOs are inconsistent. Several CEOs believe it is worth studying whether we can enhance the information sharing process by bringing together CEOs and IC leaders.

With a goal of making information sharing easier in the future, some CEOs noted that they would be willing to invest time with IC leaders in a way that builds personal relationships and trust. This personal investment would be beneficial, they said, especially during emergencies, and it would assist in the development of a sophisticated "connect-the-dots" understanding of enemy capabilities, motives, and moves. As a whole, CEOs are not interested in obtaining additional classified information, but in their ongoing effort to make appropriate long-term resource allocation decisions, they are interested in threat strategies and capabilities.

B. Recommendation 2: Clarify Laws regarding Privacy and Insider Threats

The U.S. Attorney General should publish a best practices guide for employers to avoid being in conflict with the law. This guide should clarify legal issues surrounding the apparent conflict between privacy laws and counter terrorism laws involving employees.

The rights of citizens and the needs of security for the homeland must be balanced and critical infrastructure CEOs need a clear legal environment in which to operate. These CEOs also need clear guidance that protects employee privacy while protecting their organizations and the nation from "insider threats."

C. Recommendation 3: Build on Existing Mechanisms

Leverage existing information-sharing mechanisms as clearinghouses for information to and from critical infrastructure owners and operators.

The government cannot possibly know all possible sector interdependencies, but SCCs and Sector-Specific Agencies (SSAs) can assist the government in determining which owners and operators will "need to know." At a minimum in the case of a threat, the government should notify the Partnership for Critical Infrastructure Security (PCIS) and any affected SCC. Now that the critical infrastructure owners and operators have self-organized into SCCs, and the SCCs have self-organized into the PCIS for cross-sector coordination, many sector companies turn to their SCC with questions in case of a threat. While the PCIS is in the best position to share threat and alert information with those sectors it knows the threats could possibly affect, it is also able to protect sensitive information.

Most critical infrastructure sectors have also established ISACs. However, since not all the sectors have these centers, the Council recommends that the government make its initial notification to the PCIS and any affected SCCs, since these groups will know which sectors will use their ISACs for advisory dissemination and incident response, and they will coordinate expeditiously.

DHS should fully document the differences among the sectors and it should keep them updated on a regular basis. DHS should also inform the IC of the existence of CIPAC and its subordinate organizations, and the government should work within this Sector Partnership Model.

CIPAC (including PCIS and the SCCs), ISACs, and HSIN are all gaining in effectiveness through increased participation and usage. The government should use these groups to avoid scattershot requests to the private sector through multiple government agencies and private sector associations. The DHS LLIS report also reinforces this recommendation[4]

DHS has made significant strides in enhancing information sharing through HITRAC, HSIN, NICC, PCII, and CIPAC. DHS should leverage these mechanisms as they mature, before considering creating new mechanisms or architectures.

D. Recommendation 4: National-level Fusion Capability

Establish or modify existing government entities to operate a national- and state-level intelligence and information fusion capability focused on CIP.

[4] *Ibid.*, p. 3

Fusion centers, whether physical, virtual, or a combination of the two, would benefit the IC as well as the public and private sectors, including the SCCs, SSAs, intelligence agencies, DHS, state Homeland Security Advisors, and Federal, State, local, and tribal law enforcement agencies. Services to these customers would include Request-For-Information (RFI) vetting and coordination, collaborative analysis, and timely dissemination of information across the full spectrum of CIP – from strategic planning and risk analysis to protection and deterrence, to response and recovery. Effective fusion capability includes resident or available access to experts in physical, cyber, and human aspects of CIP. The personnel involved should have reach-back capabilities to experts and data in their "home" sectors or agencies, and thus be able to amplify the requirements and analysis capabilities of the centers.

Although these centers would need to operate at multiple levels of security, they should develop, analyze, and disseminate intelligence at the lowest possible level of classification, with a strong bias toward open-source information. A guiding principle should be rapid, broad dissemination of intelligence for CIP decision makers, at the unclassified level.

The HSAC described an effective Homeland Security Intelligence and Information Fusion capability in April 2005. Even though the HSAC did not make a specific recommendation in that report, the Council endorses the principles and functions it contains.

> *The President and the U.S. Congress have directed that an information sharing environment (ISE) be created in the next two years to facilitate information sharing and collaboration activities within the Federal Government (horizontally) and between Federal, State, tribal, local, and private sector entities (vertically). The concept of intelligence/information fusion has emerged as the fundamental process (or processes) to facilitate the sharing of homeland security-related information and intelligence at a national level, and, therefore, has become a guiding principle in defining the ISE.*[5]

According to the Intelligence and Information Sharing Initiative report from the HSAC, effective intelligence/information fusion requires the following:

- The use of common terminology, definitions, and lexicon by all stakeholders;
- Up-to-date awareness and understanding of the global and domestic threat environment;
- A clear understanding of the links between terrorism-related intelligence and non-terrorism-related information (e.g., flight school training, drug trafficking) so as to identify those activities that are precursors or indicators of an emerging threat;
- Clearly defined intelligence and information requirements with the Federal intelligence community that prioritize and guide planning, collection, analysis, dissemination, and reevaluation efforts;

[5] "Intelligence and Information Sharing Initiative: Homeland Security Intelligence & Information Fusion," HSAC, April 28, 2005, p. 2 (http://www.dhs.gov/dhspublic/interweb/assetlibrary/HSAC_HSIntelInfoFusion_Apr05.pdf)

- Identifying critical information repositories[6] and establishing the processes, protocols, procedures, and technical capabilities to extract information and/or intelligence from those repositories;
- Reliance on existing information pathways and analytic processes as possible;
- All-hazards and all-crimes approach to defining information collection, analysis, and dissemination;
- Clear delineation of roles, responsibilities, and requirements of each level and sector of government involved in the fusion process;
- Understanding and elimination of impediments to information collection and sharing (i.e., it should be a priority for the Federal Government to provide State, local, and tribal entities unclassified terrorism-related information/intelligence so that it can be integrated into statewide and/or local fusion efforts);
- Capacity to convert information into operational intelligence;
- Extensive and continuous interaction with the private sector and with the public at large;
- Connectivity (technical and/or procedural) with critical intelligence streams, analysis centers, communication centers, and information repositories at all levels of classification as necessary;
- Extensive participation of subject-matter experts (SMEs) in the analytical process; and
- Capacity and commitment to ensure aggressive oversight and accountability so as to protect against the infringement of constitutional protections and civil liberties."[7]

E. Recommendation 5: Staffing

Within key intelligence agencies throughout the IC, create "sector specialist" positions at both the executive and operational levels, as applicable. Since agency directors rotate into and out of their positions frequently, these specialists should be civil servants who can develop a deep understanding of their private sector partners. DHS has accomplished this at the operational level, but the Council recommends that the department also complete this at the executive level. At a minimum, DHS and ODNI should create these positions within their respective organizations.

At the operational level, sector specialists would be analysts that develop relationships with key critical infrastructure operational decision makers, and would study the sector to develop an in-depth knowledge of its needs for information and abilities and challenges regarding dissemination.

At the executive level, sector specialists would advise agency directors regarding the need of private-sector executives to have strategic information and intelligence. They would also advise directors on private sector business continuity capabilities, limitations, and resource planning. At this level, sector "specialty" could be a collateral duty. That said, it is important to establish

[6] These repositories are not limited to those maintained by law enforcement entities. For example, critical information may be contained in systems supporting medical examiners (unattended death), public health entities, emergency rooms (information similar to the Drug Abuse Warning Network program), environmental regulatory inspectors, transportation entities, housing inspectors, health inspectors, building code inspectors, etc.
[7] *Ibid.*, p. 4

continuity within the IC of senior civil servants who are familiar with the private sector and who can establish and maintain strong relationships with critical infrastructure CEOs.

F. Recommendation 6: Training

Develop an ongoing training and career development program for sector specialists within intelligence agencies. Developing a training and career development program would allow sector specialists to maintain up-to-date knowledge regarding their target sectors' technologies, business practices, security concerns, capabilities, and limitations. DHS should establish this training program to complement Recommendation #5 above.

As part of its Lessons Learned Information Sharing (LLIS) initiative, DHS found the following:

> *Domestic intelligence sharing is currently a predominantly law-enforcement function; whereas state, local, tribal, and private sector entities would prefer a broader, more inclusive homeland security intelligence-sharing framework. Law enforcement agencies should naturally play a central role within any domestic homeland security information and intelligence-sharing framework. However, public safety disciplines such as public health, fire, emergency medical services, and private sector security provide different types of information and different perspectives that are essential for this framework to be effective. Several SMEs cited the overall lack of inclusion of these other disciplines at all levels as a critical shortcoming in the development of comprehensive, effective information and intelligence sharing processes.*[8]

Also in its report, LLIS went on to recommend that, "DHS should support the expansion of homeland security intelligence sharing and analyst training to include all public safety and works disciplines, including critical private sector entities."[9]

The Council endorses the LLIS report in its entirety. Regarding this recommendation, if DHS implements a CIP-focused training program for intelligence analysts, it should also include training on private sector information requirements and capabilities to improve analysis and dissemination for critical infrastructure stakeholders.

G. Recommendation 7: RFI Process

Establish a formal, comprehensive CIP intelligence and information requirements process. Acknowledging the diversity among sectors, The IC should tailor information gathering and dissemination to the needs of each sector and State, local, and tribal security partners. The process should provide RFIs to the IC from critical infrastructure stakeholders. In concurrence, the Council quotes portions of the first recommendation from the HSAC's Information Sharing Final Report:

[8] "LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process," DHS, December 2005, p. 4
[9] *Ibid.*, p. 5

DHS and the Private Sector should work in collaboration to develop a formal, and objectively manageable, homeland security intelligence/information requirements process.

The process should place a premium on, and leverage, superior Private Sector information resources, expertise in business continuity planning, and understanding of the operations of infrastructure sectors.

The process must recognize the diversity of the Private Sector.

The Private Sector and DHS need to integrate and align their requirements for information collection and sharing.

Information Sharing & Analysis Centers (ISACs), Sector Coordinating Councils (SCCs) and other Private Sector organizations and stakeholders must coordinate their efforts and define Private Sector requirements for DHS so that specific Private Sector entities can formally request, track and receive only that information requested. This will require doing a better job of articulating what types of information they want from government and with what frequency.

The process should include a greater bias toward disseminating more information in unclassified form. The solution should not primarily be to investigate more people and issue more clearances.

Where information must be classified, DHS and other agencies should work harder to produce unclassified versions.

The President should continue to implement on a timely basis the provisions of the Intelligence Reform law designed to expedite the clearance process.[10]

The Council recommends establishing a formal policy and supporting mechanisms for researching, vetting, requesting, prioritizing, and tracking RFIs between the IC and the private sector. Mechanisms must address timeliness, emergencies, confidentiality, FOIA, identity, and regulatory protection. DHS must integrate the RFI prioritization process with national risk management priorities. Moreover, DHS must ensure that the private sector can easily understand any RFI format. Additionally, DHS must make RFIs widely available and flexible as to form, while supporting a common understanding of function. The process must be designed to support the different requirements of pre-event (weighted towards intelligence for risk management) and post-event (more balanced intelligence and operational information needs to support re-ordered risk assessments and consequence management and recovery) information needs. In order to provide context to improve understanding of the request, RFIs should include information about how respondents will use them as well as information that identifies those who will use a response.

[10] Homeland Security Information Sharing between Government and the Private Sector, HSAC, August 10, 2005, p. 5

Now that it is established, the CIPAC should be an appropriate vehicle for coordinating the development of the needed bi-directional RFI process.

H. Recommendation 8: Standardize SBU Markings and Restrictions

The Federal government should rationalize and standardize the use of SBU markings, especially FOUO, and publish standard handling instructions clearly for all intended recipients.

According to a recent GAO report, "GAO recommends that the Director of National Intelligence (DNI) assess progress, address barriers, and propose changes, and that OMB work with agencies on policies, procedures, and controls to help achieve more accountability."[11] The Council agrees, and additionally recommends that study participants should include senior representation from the leadership of SCCs and GCCs, as well as the affected IC agencies.

[11] *Op cit.*, GAO-06-385, p. 1

Appendix A – The CEO Perspective

A cross-section of CEOs were interviewed representing major critical infrastructure corporations, some of them NIAC members, to discuss their views on improving information sharing between the private sector and the IC to protect critical infrastructure. These interviews examined the issues of information sharing within the broader context of the chief executive's role in managing business and operational risks since the events of September 11.

The following summarizes the key findings, conclusions, and recommendations from these interviews.

A. Findings

Motivation and Limitations

The Working Group spoke informally with CEOs about their motivations and willingness to share information with the IC.

All the CEOs interviewed were clearly patriotic and expressed a sense of duty to the nation. They were all willing to be helpful. All were committed to sharing resources in response to an emergency. However, routine interactions come with cautions: the interactions need to be legal, aligned with stakeholder interests, and need to take reasonable time and resources.

Barriers to Information Sharing

The Working Group asked CEOs for their thoughts on what is most responsible for hampering information sharing today.

Though CEOs acknowledged that IC officials rarely solicit them for information, they did reflect the frustrations of their subordinates with repeated solicitations for identical information from multiple government agencies (not always intelligence agencies). These unnecessarily duplicative and repetitive requests represent an under-appreciation of the value of time to business owners and operators. In addition, CEOs regard those government requests that demonstrate a lack of knowledge about their businesses as another inefficient use of their time.

Almost all the CEOs interviewed indicated they are reluctant to share information with the government if it means more regulation.

The Council states that it is important for CEOs to understand why the government needs a specific piece of information. CEOs are willing to share information if the government can provide there is a valid reason for the government to know something. The reason that CEOs want to know why agencies are asking for information is to give better answers. CEOs understand a great deal about their businesses, and they can answer questions from dozens of different perspectives. If they recognize the goals of the information requests, they can tune their answers more effectively. They can give answers that are far more relevant if they appreciate the greater conceptual framework in which IC officials seek the information.

Many CEOs interviewed indicated that the government should be particularly careful to characterize the threat as accurately as possible. All threats cannot and should not be weighed equally, the CEOs said, adding that not all threats represent a top national priority. Those CEOs aware of Secretary Chertoff's risk-based approach applauded it. Most, however, were unaware of it.

Expectations

The Working Group asked CEOs what they expected from government and what government could reasonably expect from them.

The CEOs interviewed were very realistic about what government is likely to know and not know, and they believe that private enterprises are essentially responsible for their own resiliency. CEOs do not necessarily expect government officials to know much about their business, but they expect them to inform CEOs if the government is aware of a specific, credible threat to their employees, physical plant, or cyber assets. They also expect the government to inform them if it knows that their company has inadvertently employed a terrorist.

CEOs expect the government to be reasonable in its demands and to recognize that companies cannot possibly defend against every possible threat. CEOs take calculated risks every day, and those who operate international and multi-national operations must deal with serious risks overseas on a daily basis. To that end, CEOs expect the government to set the public's expectations about the long-term nature of the threat.

Many CEOs expressed the feeling that neither government nor industry has the ability to protect everybody against everything. Rather, the burden, they said, is a shared and sustained burden and one in which all partners have a significant stake and role.

The CEOs also commented about what government should expect from industry. The executives noted that good citizenship requires cooperation and responsiveness to reasonable, specific, sophisticated queries from intelligence agencies. These queries, they added, must always be within the law, and within the corporation's responsibilities to its various stakeholders.

Reasonableness

CEOs recognize industry needs an understanding with the government about striking a reasonable balance between preventive hardening, on the one hand, and recovery and resilience, on the other.

Government calls for "hardening" corporate infrastructure are not supported by information that indicates known terrorist groups are threatening domestic assets: To date, most companies have internalized the consequences of 9/11 into their risk management and business continuity plans, based on risk assessments initiated and conducted by the companies themselves. Companies typically initiated these actions without government assistance. Executives indicated that if the government believes the private sector needs to do more at the *preventive* end of the spectrum, it must present companies with specific and credible threat information. They added that credible information would reveal that identifiable terrorist groups have targeted infrastructure assets. In the absence of such information, CEOs said their companies would rely more on response and

recovery actions rather than protective measures to address the remote risks of terrorist attack. While the risk that terrorists will once again launch an attack within our borders remains high, the executives maintained that the risk that a particular private sector site will be hit remains low.

Personnel security is a vital component in protecting critical infrastructure from insider threats; however, privately investigating employees does not completely prevent highly sophisticated terrorists from infiltrating company work places. Several of the executives expressed frustration over the mismatch in federally mandated obligations to vet personnel and customers and industry's ability to know enough about employees and customers to do a thorough job vetting them. Compounding this is the equally important principle of protecting employees' privacy. While CEOs felt responsible for protecting their employees' privacy, they felt equally responsible if one of their employees turned out to be an internal threat that a screening might have prevented. The underlying request for CEOs is to allow the government flexibility in interpreting the law. This flexibility would allow Federal officers to exercise judgment as they fit enforcement to circumstance.

Shared investment

As follow-on to the discussions about what government should expect of business, the Working Group asked CEOs whether they were willing to invest time and effort into sharing information with the government. The answer was, "Yes, to a point."

In the heat of an emergency, they will help in whatever ways they can. CEOs stressed their willingness to train intelligence professionals about their industries on a routine basis. In many cases, industry-specific knowledge, they said, is the key to a successful "connect-the-dots" analysis.

Some CEOs indicated that they were willing to come to Washington, D.C. occasionally to meet with IC leadership in order to develop personal relationships and improve the trust that may be useful in emergencies later.

Other CEOs said they were willing to provide government with subject-matter expertise on a reasonable basis. This willingness varied by sector and contractual or legal obligations. In some cases, experts could be "on call" in the event of an emergency. In others, virtual response mechanisms would be more appropriate, the executives noted.

Perspective

The Working Group asked CEOs what they expected in return from the government for sharing information with the IC.

The CEOs interviewed are interested in the "big picture" issues of the long-term struggle with terrorists. They want to know how terror tactics and methods have changed and why, and they want to understand the motives of potential attackers. They want to know whether the threat in the United States is shifting from targets that are "iconic" (i.e., the World Trade Center) and "pillars of the economy", (i.e., oil fields) to other so-called "soft" targets, such as shopping malls and theaters.

It would be helpful to the private sector if IC officials alerted CEOs about issues they should be on the lookout for that might signal a threat. When a perceived threat arises, CEOs want the assurance there is someone they can call to get the answers to their questions. The individual on the other end of the line should, they said, be their peer in judgment, responsibility, and authority.

Of note, the executives maintained that they did not need access to classified information, unless it pertained to a direct threat to their business, or unless the information provided necessary context that would change the answer to a question the government is asking them.

Trust

The Working Group asked CEOs about the role of personal relationships and trust in information sharing.

The CEOs agreed that conversations among people who already know and trust each other are more fruitful than conversations among people who do not trust each other. Therefore, in order to develop trusted relationships with their private sector counterparts, senior intelligence officers should invest time and effort with key CEOs in each sector, the executives noted.

However, because individuals in both the public and private sector rotate into and out of positions, personality-based trust is not sustainable. A process in which CEOs and senior career intelligence officers have a chance to meet each other and build personal relationships is required. In addition to developing personal relationships, CEOs said that a defined relationship-building process was vital for sustained effective information sharing.

Information sharing will continue to remain a tactical activity conducted by mid-level government and industry security professionals. These professionals cannot authoritatively address, let alone decide, matters of strategic policy or resource allocation. Therefore, high-level trusted relationships and processes must support those kinds of decisions made by chief executives and senior government policy officials.

Governance

The Working Group asked CEOs if infrastructure protection and information sharing issues rose to the level requiring the attention and concern of a company's Board of Directors.

The CEOs said that the day-to-day management of security issues rarely reaches the board level. Moreover**,** executives reported that boards of directors rarely consider security issues at meetings, except when members raise such issues in the context of reviewing a company's overall business and risk management practices. **However, boards of directors traditionally are deeply involved in security controls, especially as they involve audits. Boards often review business continuity plans, including exercises and dry runs.**

Companies have built resilience for many kinds of threats into their business practices. Resilience is a lot less expensive than trying to protect against all threats. Over time, resilience issues are addressed by a company's management, not its board of directors.

Incentives

The Working Group asked CEOs whether the private sector has sufficient incentive to invest in infrastructure protection and to share information with its government partners.

Not surprisingly, the executives' answers revolved around competition, citizenship, and long-term self-interest. On the one hand, competition drives CEOs to protect their infrastructures. On the other hand, citizenship and enlightened self-interest spurs them to share information with government agencies. Many of the CEOs interviewed manage truly global companies and have the ability to shift production outside the United States if unreasonable security demands increase costs on U.S. facilities.

CEOs indicated that the Americans with the greatest stake in protecting against terrorist attacks are those employees who work at facilities that are potential targets. For example, in the food industry, a biological threat introduced into a batch of food would undoubtedly lead to the plant's closure and the local workers would be out of work. The executives were quick to point out that these same local workers on the front lines of the intelligence battle. By virtue of their daily routine, these employees, according to the conversations, are also the most likely to recognize that "something is wrong" or that "someone is new" within their environment. Creating a low-level, constant public awareness of the possibility of terrorist actions should have a positive effect in plants across the country, the CEOs said.

Strengths and Weaknesses

The Working Group asked CEOs about the relative strengths and weaknesses of government in protecting infrastructure.

Most executives believe the government, and specifically the IC, is in the best position to inform the private sector on physical threats to infrastructure due to its superior ability to collect and analyze information on terrorist groups worldwide. However, few executives believe the government can provide the same level of timely value-added information on cyber threats. In fact, most CEOs maintained that private industry is far more likely and able to discover and mitigate cyber threats than the government.

B. Conclusions

In order to help protect the country from terror threats and attacks, the CEOs interviewed for this study are capable and willing to share information and cooperate with the IC, but they have their limitations. Partnership with government cannot undermine shareholder value or damage customer confidence, and it must operate within the law.

Critical infrastructure CEOs have a great deal of experience developing and managing working relationships with other entities. Clear definitions of the goals of the working relationship and the obligations of each participant need to be spelled out, with full knowledge that the critical element is enough trust in the goals and the intentions of each party to allow for change as time passes and needs change.

CEO responses reflected their perspective regarding the private sector's partnership with government, in general. More specifically, the responses highlighted their thoughts regarding intelligence coordination. The Council established four conclusions from their discussions with the CEOs:

1. **Private sector CEOs will share information and cooperate if their sharing and cooperation is legal and is consistent with the interests of their corporate stakeholders.**

2. **Private sector CEOs will invest time to meet and develop trusting relationships with intelligence officers of commensurate responsibility and authority. They are also supportive of establishing a process-based approach to building trust between the two parties.**

3. **Each of the 17 CI/KR sectors has differing cultures and vocabularies. The intelligence community needs to understand the formal and informal communications hierarchies within each sector, including the roles of important players.**

4. **Intelligence officers would receive more complete and relevant answers from their private sector counterparts if they provided deeper context for their questions.**

Appendix B – Case Studies

1. Purpose

To illustrate the issues and findings addressed by the NIAC Intelligence Coordination effort, the Study Group conducted case studies on four recent significant incidents involving critical infrastructures and the IC. The purpose of these case studies was to trace key pieces of information from their sources to decision makers. Moreover, these cases either highlight the value of that information in decisions made or underscore the gaps in the information-sharing process. Organizers did not design these case studies to assign blame. Instead, they support the Study Group's findings and offer a way to improve coordination between the IC and critical infrastructure owners and operators.

2. Cases

The selected cases represent very different events. Organizers strived to ensure that the cases represented an all-hazards approach to CIP and that all aspects of information sharing were covered. Two of the four events occurred before public and private partners shared any information, so the lessons learned are in the realm of *post-event analysis*. The other two cases, which involve warnings to critical infrastructures based on intelligence analysis, represent *pre-event preparation*. Three of the four cases related to a terrorist act or an intended attack while the fourth was a non-hostile event. The four cases were:

1. Blackout, August 2003
2. Financial Services Threat Alert, July 2004
3. London Bombings, July 2005
4. New York Public Transit Threat Alert, October 2005

3. Structure

Each case study begins with a short summary of the event. A tabular representation of a timeline (all times Eastern Time) follows the summary. The timeline includes when information was shared, by whom and with whom it was shared; which key decision makers were involved in the sharing of information, and what key decisions were made as a result. Finally, each case study includes a conclusion that highlights information-sharing lessons learned, and relates those lessons to the overall Study Group findings.

A. Blackout, August 2003

Summary

"On August 14, 2003, large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power blackout. The outage affected an area with an estimated 50 million people and 61,800 megawatts (MW) of electric load in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey and the Canadian province of Ontario. The blackout began a few minutes after 4:00 pm Eastern Daylight Time (16:00 EDT), and officials did not restore power for four days in some parts of the United States. Parts of Ontario suffered rolling blackouts for more than a week before authorities could fix the

problem. The estimated total costs from the blackout in the United States ranged between $4 billion and $10 billion (U.S. dollars).[12] In Canada, gross domestic product was down 0.7 percent in August, there was a net loss of 18.9 million work hours, and manufacturing shipments in Ontario were down $2.3 billion (Canadian dollars)."[13]

There were concerns in the subsequent investigation regarding whether the blackout was caused, in whole, or in part, by an intentional act, either physical or cyber. Led by a team from the CERT® Coordination Center (CERT/CC) at Carnegie Mellon University and the Royal Canadian Mounted Police (RCMP), the Cyber Analysis sub-team analyzed and reviewed electronic media of computer networks in which online communications take place. The sub-team examined these networks in an effort to determine if someone or some group used them maliciously to cause or contribute to the outage. Specifically, the Security Working Group (SWG) reviewed materials, created on behalf of DHS' National Communication System (NCS), which included the team's analysis and conclusions of its Internet Protocol (IP) modeling correlation study of Blaster (an Internet worm first noticed on August 11, 2003) and the power outage. "This NCS analysis supports the SWG's finding that viruses and worms prevalent across the Internet at the time of the outage did not have any significant impact on power generation and delivery systems. The team also conducted interviews with vendors to identify known system flaws and vulnerabilities."[14]

> *The Intelligence Analysis sub-team was led by DHS and the RCMP, which worked closely with Federal, State and local law enforcement, intelligence and homeland security organizations to assess whether the power outage was the result of a malicious attack. SWG analysis provided no evidence that malicious actors—be they individuals or organizations— were responsible for, or contributed to, the power outage of August 14, 2003. Additionally, the sub-team found no indication of deliberate physical damage to power generating stations and delivery lines on the day of the outage and there were no reports indicating the power outage was caused by a computer network attack.*[15]

Timeline

The timeline below lists all the key communications related to the August 14, 2003 power outage that case organizers could collect. The ESISAC coordinated and responded to much of the communication in the immediate aftermath of the outage and in the days immediately following the outage. There were many individual communications seeking specific information during this time, but organizers did not record them here. Detailed information pertinent to the outage including the final report with causation and recommendations is available at www.nerc.com.

---

[12] See "The Economic Impacts of the August 2003 Blackout," Electric Consumer Research Council (ELCON), February 2, 2004.

[13] Statistics Canada, *Gross Domestic Product by Industry*, August 2003, Catalogue No. 15-001; *September 2003 Labour Force Survey*; *Monthly Survey of Manufacturing*, August 2003, Catalogue No. 31-001.

[14] p. 133-134 U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, p. 1.

[15] *Ibid.*, p. 134

Abbreviations used:

APPL	New York City Police Department (NYPD) Area Police/Private Security Liaison (communication mechanism between NYPD and New York City private security directors—primarily e-mail, with phone and physical meetings as backup)
BES	Bulk Electric System
BID	New York City Business Improvement District (localized private security patrols designed to give a visible security presence in dense business areas)
CIPAG	(NERC) Critical Infrastructure Protection Advisory Group (now CIP Committee)
DHS	Department of Homeland Security
DOE	Department of Energy
EEISC	Edison Electric Institute Security Committee
ESISAC	Electricity Sector Information Sharing and Analysis Center
FERC	Federal Energy Regulatory Commission
IT-ISAC	Information Technology Information Sharing and Analysis Center
MS-ISAC	Multi-State Information Sharing and Analysis Center
NERC	North American Electric Reliability Council
RC	Reliability Coordinator (17 operation centers coordinate bulk electric system operations U.S. and Canada)

Communications mechanisms included the RC hotline (a blast bridge facility), dial-in conference calls, point-to-point telephone calls, secure telephone calls (STU-3), and email.

Time (EDT)	Contacts	Content
Thursday, August 14, 2003		
1505		Initial events (outages) that led to the cascading separation
1505 -1610	Bulk electric system operators	Numerous telephonic contacts among bulk electric system operators. Numerous bulk electric system events.
1610		Final bulk electric system separation
1610 +	RCs and ESISAC hotline	First information gathering call
~1620	APPL	Activated using a back-up computer server. Test message sent to subscribers, followed by NYPD assessments of the situation. Advisory to members stating that extra NYPD APPL staff was operating APPL, and could be contacted by e-mail or phone.
~1640	APPL	All reporting assets (to NYPD) were dismissing terrorism as the cause of the blackout
not rec	APPL	Advisory that Consolidated Edison had advised NYPD of strong possibility of rolling blackouts throughout the city over the weekend. APPL strongly recommended all businesses consider extra security

1915	**RCs, ESISAC, Agencies hotline**	**These calls were conducted frequently during the first several days of the outage. The RCs and ESISAC participated on all calls. DHS, DOE, and FERC participated on most calls. The call format was:** **1. Status of restoration** **2. Stability of bulk electric system** **3. Damage report** **4. Any other challenges** **5. Causations** **6. Any RC needs.**
not rec	APPL	Advised increased security presence for BIDs
not rec	ESISAC	Initial call to ST/PT-ISAC
2200	RCs, ESISAC, Agencies hotline	
2310	IT-ISAC	IT-ISAC sent email to the ISAC Council with IT related discussion points
Friday, August 15, 2003		
0004	RCs, ESISAC, Agencies hotline	
not rec	IT-ISAC	Requested collection of data from members on two areas: 1) blackout; 2) impact of Blaster worm. Received information back from several, and from MS-ISAC.
0040	IT-ISAC	Though officials do not believe the Blaster Worm caused the outage, it is under investigation. Advisory of possible future impact of a worm attack leading to denial of service
0500	RCs, ESISAC, Agencies hotline	
0600	ESISAC and White House Situation Room	Briefing at the SECRET classified level regarding the outage extent, causation factors known at this time, restoration progress
0600	NERC and media	Internet posted update
0800	RCs, ESISAC, Agencies hotline	
0845	FS-ISAC/Treasury and ESISAC tel call	RFI from FS-ISAC with response subsequent
0845	NERC and media	Internet posted update

not rec	**NERC**	**Commenced the formal outage investigation involving all systems affected by the outage, agencies of the United States and Canada, and Electricity Sector subject-matter experts. This investigation, evaluation was one of the most intense such studies ever undertaken. The results are included in the formal report, noted above in the lead paragraph**
1030	Impacted utilities and ESISAC	Detail discussion on aspects of restoration
1100	NERC and media	Internet posted update
1115	EEISC and ESISAC conference call	Discuss outage status in manner similar to the RC calls
1200	RCs, ESISAC, Agencies hotline	
1245	NERC and media	Internet posted update
1255	Impacted utility and ESISAC	Detail discussion on aspects of restoration
1315	CIPAG and ESISAC conference call	Discuss outage status in manner similar to the RC calls
1400	Comm ISAC and ESISAC tel call	RFI (request for information) from Comm ISAC
1424	Comm ISAC and ESISAC tel call	RFI response
not rec	ST-ISAC and ESISAC tel call	Outage discussion
1600	RCs, ESISAC, Agencies hotline	
1630	NERC and media	Internet posted update
1645	DHS and ESISAC	Update
not rec	DHS and ESISAC	Commence the cyber investigation led by DHS
Saturday, August 16, 2003		
	RCs, ESISAC, Agencies, Others	Conference calls were conducted as on Friday
1000	ESISAC conference call	Coordinated set up of the Electricity Sector participants in the cyber investigation
not rec	NERC	A letter was sent by NERC requesting specific data retention for the physical and cyber investigations
1430	DOE and NERC tel call	
Sunday, August 17, 2003		
	RCs, ESISAC, Agencies, Others	Conference calls were conducted as on Friday
1000	Impacted utility and ESISAC	Detail discussion on aspects of outage

1045	DHS and ESISAC	Prepare for commencement of cyber investigation
1100	Cyber Investigation Team conference call	Commence cyber investigation
Monday, August 18, 2003		
	RCs, ESISAC, Agencies, Others	Conference calls were conducted as on Friday, at reduced frequency
1115	DHS, DOE, ESISAC daily security briefing conference calls resumed	
1145	U.S. Secret Service and ESISAC	Outage briefing
1315	Specific utilities and ESISAC	Restoration and outage study discussion
not rec	Specific utility, Comm ISAC, ESISAC	RFI and discussion
not rec	APPL	As power was gradually restored, issues status reports of various mass transportation systems serving New York City
Tuesday-Friday, August 19-22, 2003		
	Routines including media contacts continued at reduced frequency.	Outage investigation well underway
not rec	APPL	Summary message stating blackout was over, including observations regarding what might be done if another blackout were to occur

Conclusions

It became clear early on August 15, 2003 that coordination between the Electricity Sector Information Sharing and Analysis Center (ESISAC) and the Information Technology Information Sharing and Analysis Center (IT-ISAC) provided enough assurance to electric sector investigators to allow them to focus on physical causative factors and restoration. The cyber investigation led by DHS confirmed these initial findings. DHS and law enforcement officials, as well as IC analysts, concluded there was no indication of malicious activity - either physical or cyber - connected with this incident. While the presence of Blaster on the Internet and business systems across the country added to initial anxiety, it was determined that the worm did not contribute to this incident.

Two lessons learned in this case are applicable to intelligence coordination. First, existing communication architectures among private sector organizations are useful for sharing information and analysis. Second, the private sector possesses a profound understanding of cyber

security. Subject-matter experts can analyze network information quickly and accurately to support analysis. These conclusions support the Study Group findings regarding the need for:

- trusted relationships between the IC and critical infrastructure owners and operators;
- education for IC analysts that covers private-sector capabilities and leverages private sector subject-matter expertise as appropriate; and
- a streamlined RFI process that provides an open and timely exchange of information between the IC and the private sector.

B. Financial Services Threat Alert, July-August 2004

Summary

During late July 2004, analysis of, in the words of DHS, "credible and specific intelligence reporting" indicated that terrorist operatives had conducted extensive research and reconnaissance activity against major U.S. and international financial institutions in Washington, D.C., Northern New Jersey and New York City. DHS issued warnings to specific entities and raised the threat level to "Orange—High" for the Financial Services Sector in those three specific regions. The named entities included the Citigroup buildings in and around New York City, the New York Stock Exchange building in Lower Manhattan, the International Monetary Fund and World Bank buildings in Washington D.C., and the Prudential Insurance Company of America in Newark, New Jersey. The reporting provided a level of detail that was unusually specific, including information about the interior configurations of these buildings, as well as infrastructure, services, and buildings that surround them.

Initially, officials stated that the newest information came from a Pakistani computer engineer who authorities had captured the previous month. Actually, intelligence officials had culled much of the information years earlier, even before September 11, 2001. The alert did not specify a timetable for the possible attack.

Various private meetings and public statements ensued, prompting security directors of the named entities and several other institutions, as well as law enforcement officials to implement preventative measures. These measures remained in effect until November 10, 2004, when the DHS Secretary lowered the threat level for these specific targets and the sector to "Yellow—Elevated."

Timeline

Abbreviations used:

AAR	Association of American Railroads
APPL	NYPD Area Police/Private Security Liaison (communication mechanism between NYPD and New York City private security directors—primarily e-mail, with phone and physical meetings as backup)
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council
JTTF	Joint Terrorism Task Force
NEXUS	NYPD program centering on personal contact with New York businesses,

including information on "terrorist indicators" to watch for, literature, signage to post, and contact information

RE-ISAC Real Estate Information Sharing and Analysis Center

ST-ISAC Surface Transportation Information Sharing and Analysis Center

Time (EDT)	Contact	Content
Thursday, July 29, 2004		
not rec	IC	Began sharing intelligence including evidence of terrorist observation of traffic patterns, guards, cameras, and garages for the targeted buildings.
not rec	JTTF New York Field Office	Principals-only cabinet-level meeting with NYPD Police Commissioner, Deputy Commissioners of Intelligence and Counter Terrorism. Outlined information developed over last few days regarding Al Qaeda-linked reconnaissance information shared within broader federal IC and NYPD, and including terrorist observations of traffic patterns, guards, cameras, and garages for the targeted buildings
1509	AAR Ops Center	Advisory to railroads based on open-source information, warning of general threats to metropolitan areas of NY, DC, Las Vegas, and Los Angeles—recommended heightened vigilance
Friday, July 30, 2004		
not rec	NYPD	Informed specific companies and institutions connected with the New York City named buildings
not rec	DHS Secretary Ridge	Called CEOs of named institutions in New York City
Saturday, July 31, 2004		
not rec	APPL	Message to APPL members advising them of threat and outlining known details. Through the day and following days, transmitted specific advisories of what indicators might precede such an attack, along with "best practice" advice on hardening possible targets
not rec	Security Directors	Most financial and real estate sector security professionals had much of the story, spread among security directors as they saw need.
not rec	NEXUS	Focused on businesses involved in truck, van, and limousine rentals based on specific information regarding intelligence on terrorist attack methods
Sunday, August 1, 2004		
Morning	NYPD	Police Commissioner Kelly met in person with the security directors of 13 major financial institutions in the New York area to discuss the threat, as well as to review security measures initiated by the Police Department and the private sector in response. A message regarding this meeting was transmitted.

Morning	**FBI**	**Detailed briefing for institutions named in the intelligence regarding the New York City buildings. At that meeting, the private sector security directors communicated the importance of sharing the info with the security for the Citicorp Center – its owner and manager, Boston Properties. (At that time, Citicorp neither owned managed or even occupied a majority of the Citicorp Center. It was, therefore, not responsible for perimeter security.)**
1245	DHS	Assistant Secretary for Infrastructure Protection Robert Liscouski holds a briefing for ISACs and Sectors detailed evolving situation, unprecedented to have specific information. Some non-financial sector reps asked whether DHS was warning other collocated sector facilities (telecom, electric, transit). Liscouski said that DHS was not.
1300	DHS	Secretary Ridge – National press conference[16] – FS Sector alert level raised to Orange for NY, N.J. and Washington, D.C. "Background Press Briefing by DHS by Senior Intelligence Officials" provided[17]
not rec	New York State Office of Homeland Security	Relayed DHS advisory titled "Threat Alert Level Increased to Orange For Financial Services Sector in new York city, Northern New Jersey, and Washington, DC." Included same text sent earlier by NYPD regarding how best to harden possible targets
not rec	DHS	Issued advisory to sectors and ISACs following press conference
1513	ST-ISAC	Forwarded DHS advisory to members immediately after receipt
1900	FS-ISAC	Alert sent to members
not rec	FS Sector Coordinator Donahue	Conference call with Under Secretary Abernathy, U.S. Treasury, FSSCC, and FS-ISAC members
not rec	NYPD, Security Directors	Carried out extra bag and identification checks across the cities during the week of August 1, while police officers and bomb-sniffing dogs milled outside of office buildings. Authorities close some bridges and tunnels in New York to trucks. Police set up metal fences surrounding the headquarters of Prudential Financial, blocked off two streets, and armed themselves with assault rifles.
Evening	DHS	Joint DHS/FBI Advisory to the FS-ISAC and RE-ISAC—far less detailed than publicly released background briefing, except that it named the specific buildings of interest

[16] http://www.dhs.gov/dhspublic/display?content=3870
[17] http://www.dhs.gov/dhspublic/display?content=3872

Monday, August 2, 2004		
1415	FS-ISAC	Conference Call with Undersecretary Wayne Abernathy on Recent Threats to Financial Sector
Tuesday, August 3, 2004		
	DHS Secretary Ridge	Met with selected financial institution security directors, including NYSE, at Citicorp headquarters. Separate meeting with senior security executives from 5 or 6 major financial institutions. At this second meeting, the security directors strongly recommend an earlier "heads up" on issues of this magnitude. The point was made that individual named companies were briefed, but the publicly announced change in threat level was for the entire financial sector. Therefore, authorities needed to advise a broader set of security professionals before the public change in the nation's posture.
Tuesday, November 9, 2004		
not rec	APPL	In-person meeting in NYPD Headquarters auditorium discussing upcoming Republican National Convention, and congratulating all on response to the threat
Wednesday, November 10, 2004		
2053	FS-ISAC	DHS Lowering Threat Level For Financial Institutions in NY, N.J., and Washington, D.C.

Conclusions

This incident highlighted some of the challenges local officials face when they have to decide what kind of information to act on and what information to make public. It also underscored the importance and challenges that the government faces in its communications with the private sector before major public announcements. Employees of large financial institutions and the thousands of occupants of large buildings were unnerved to learn of the threats in the press. In this case, the amount of highly detailed information shared with the press was extensive and the news surprised most of the financial service building owners and managers. Therefore, the owners and managers were not in a position to advise their employees promptly about the steps they were taking to protect them in their workplaces.

This case clearly shows the pressure that local governments feel to promptly "come clean" with the public in the face of provocative information. Similarly, financial sector and commercial sector security officials feel a practical pressure to communicate quickly and definitively with their constituents. Therefore, when the Federal government shares information this precise and this explosive with local governments, officials should assume the information will eventually

become public. With knowledge that the public will soon be aware of the threat, officials should share the information with relevant private sector security officials, including critical infrastructure owners and operators who are collocated or in close proximity to affected sites as quickly as possible after advising local authorities.

Another important lesson from the incident arose from the fact that DHS officials assumed Citicorp owned, managed, or otherwise had responsibility for security at the Citicorp Center. In fact, companies often pay to place their name on a building for advertising purposes even if they do not actually own the building. Moreover, building owners often name their buildings for companies that no longer own or never did own, manage, or even occupy significant parts of the facility. Therefore, early on in any advisory process, government officials must consult with private-sector subject-matter experts to be sure they know who owns, operates, and occupies the facilities, and most importantly, who the key decision makers are that must be notified in order to take appropriate action.

In contrast to this "mistaken identity" error, NYPD has developed and maintained long-standing relationships with security directors at most of the landmark institutions around the city. In fact, many of those security directors are retired NYPD. The security directors, and NYPD itself, would usually know the appropriate decision makers for sites of interest. The lesson is that private sector owners and operators must keep appropriate authorities informed regarding changes in residence, security responsibilities, and tenancy of critical infrastructure assets.

These conclusions support the Study Group findings that:

- Trusted relationships between private sector owners/operators and the IC are key to success;
- IC analysts, including DHS and FBI officials, must rely on private sector subject-matter expertise to know who to contact with important information; and
- There is a need for a protection mechanism for highly sensitive, but unclassified information. This includes possible overlapping circles of "need to know" individuals and groups.

C. London Bombings, July 2005

Summary

On July 7, 2005, at about 08:50 local time, three explosions occurred within 50 seconds in the London subway system. A fourth explosion on a bus in Tavistock Square happened 57 minutes later. The attacks killed more than 50 people and injured more than 700. On July 21, a second set of attacks occurred when small blasts on three subway cars and one on a bus occurred during the lunch rush. There is no known link between the July 7 and the July 21 attacks.

Timeline

Abbreviations used:

AAR	Association of American Railroads
APPL	NYPD Area Police/Private Security Liaison (communication mechanism between NYPD and New York City private security directors—primarily e-mail, with phone and physical meetings as backup)
APTA	American Public Transportation Association
ASLRRA	American Short Line and Regional Railroad Association
FTA	Federal Transit Administration, U.S. Department of Transportation
HSIN	Homeland Security Information Network, U.S. Department of Homeland Security
HSOC	Homeland Security Operations Center, U.S. Department of Homeland Security
ISS	Internet Security Systems, Inc.
JTTF	Joint Terrorism Task Force
MTA	Metropolitan Transportation Authority, State of New York
NEXUS	NYPD program centering on personal contact with New York businesses, including information on "terrorist indicators" to watch for, literature, signage to post, and contact information
NICC	National Infrastructure Coordinating Center, U.S. Department of Homeland Security
RE-ISAC	Real Estate Information Sharing and Analysis Center
RISS	Regional Information Sharing Systems, U.S. Department of Justice
SHIELD	NYPD Flagship program for sharing intelligence with New York security directors
ST/PT-ISAC	Surface Transportation/Public Transportation Information Sharing and Analysis Center
SWERN	SouthWest Emergency Response Network
TSOC	Transportation Security Operations Center, Transportation Security Administration, U.S. Department of Homeland Security

The Surface Transportation/Public Transportation Information Sharing and Analysis Center (ST/PT-ISAC) sent an initial report to the field at 0558 EDT July 7, 2005.

During the July 7 incident, the first government interface with the ISAC and the AAR Operations Center occurred almost an hour and a half after the ISAC sent its initial report to rail stakeholders. The timeline also shows that certain government agencies released information to entities other than the ISAC or AAR Operations Center. Eventually, the ST/PT-ISAC received this information from other sources and then responded appropriately. The sequence of events regarding information flow for the July 21 incident is similar.

In both incidents, the initial information obtained from CNN, the ST/PT-ISAC, and AAR Operations Center proved to be sufficient to drive action by the rail and public transit sectors. Prompt follow-up phone calls from ISAC, APTA and AAR officials to various rail and transit operators confirmed that officials had put additional security measures into effect. For example, freight railroad police quickly collaborated with Amtrak and commuter rail operators to provide

immediate support in the form of extra police forces, including canine teams, to patrol major metropolitan rail stations.

Time (EDT)	Contact	Content
Thursday, July 7, 2005		
0430	APPL	Initial advisory to APPL members (Note: NYPD detective liaison to London Metropolitan Police was at Scotland Yard alongside its investigative staff—provided expedited information to NYPD. NYPD passed information to detective liaison from other U.S. law enforcement and intelligence agencies.)
not rec	APPL	Subsequent messages to APPL members saying no specific threat to NY area transit
~0530	CNN	PT/ST-ISAC employee saw news on arrival for shift
0558	PT/ST-ISAC	Initial report
0727	PT/ST-ISAC	Request from TSOC to forward Initial Report and additional information/analysis from PT/ST-ISAC
0755	Water ISAC	Initial Report
0917 0923 0932	PT/ST-ISAC Water ISAC HSIN	Follow up information Follow up information from London SWERN – Initial request to report suspicious activity
1020	HSOC	"Sec. Chertoff Code Orange Statement"
Ongoing	NEXUS	Focused on surveying sporting goods, Army/Navy, beauty supply and camping supply stores. Specific attention was given to firms selling hexamine fuel tablets, an ingredient integral to the IEDs used in the London transit bombings.
not rec	SHIELD	Full-membership briefing at Police Headquarters relaying particulars of the London event. Included details on how the bombers conducted reconnaissance of the bomb sites, how they traveled to the bomb sites, how they constructed the bombs, and the ingredients that were used
1035	RISS	Translation of internet site claiming responsibility
1154	Water ISAC	Posting information and Raising alert level
Afternoon	APPL	Relayed DHS Code Orange advisory. Followed this with Police Commissioner Kelly statement outlining NYPD actions
1229	PT/ST-ISAC	Notification of DHS Conference Call
1259	PT/ST-ISAC	Cancellation of DHS Conference Call
1301 1303 1310 1311	RISS PT/ST-ISAC HSOC- SWERN PT/ST-ISAC	Special Report London Bombings Conference Call underway London Bombing Update – No-Redistribution Posting on DHS Website – Alert Level
1333 1335	PT/ST-ISAC Water ISAC	Redistribution of "Responding to Terrorist Threat" Follow up Open Source Reporting
1400	RE-ISAC	Nationwide Conference Call including DHS
1443	Water ISAC	Redistribution of "Responding to Terrorist Threat"

1510	RE-ISAC	Alert including DHS guidance to real estate owners/operators
1811	DHS HSOC	Joint DHS/FBI Bulletin – Transit Alert Levels
1933	DHS HSOC	Joint DHS/FBI Bulletin – London Terrorist Attacks
1945	RE-ISAC	Retransmission of Joint DHS/FBI Bulletin "London Terrorist Attacks"
Friday, July 8, 2005		
0824	Water ISAC	Retransmission of Joint DHS/FBI Bulletin London Terrorist Attacks
0914	Water ISAC	Retransmission of Joint DHS/FBI Bulletin – Transit Alert Levels
1504	Water ISAC	Water ISAC Analyst Comments
Thursday, July 21, 2005		
0832	PT/ST – ISAC Water ISAC	Initial report
0843	PT/ST-ISAC Water ISAC	Information Update # 1
0845	FTA	FTA received message from MTA of CNN/Fox news reports of attacks
0908	FTA	Retransmission of PT/ST-ISAC 8:43 Message
0937	ISS Atlanta	London Attacks
0937	Inter ISAC Group	Inter ISAC Reporting begins
0940	PT/ST ISAC Water ISAC	Information Update # 2
1044	PT/ST ISAC Water ISAC	Information Update # 3
1115	DHS	DHS Conference Call Message (*Sent to APTA, AAR, ASLRRA, and various government agencies, not to transit agencies)*
1136	FTA	FTA Retransmission of DHS Conference call message
1336	PT/ST ISAC Water ISAC	Analyst Comments
1511	NICC/DHS	First Official Report from DHS

Conclusions

Critical infrastructure owners and operators usually have contingency plans "on the shelf." Indications and events can trigger preplanned actions at multiple levels of planned security. At the time of these incidents, there was no assurance that the violence would be limited to London, so railroad and public transit authorities took appropriate precautions, elevating security profiles in New York, Washington, D.C., Chicago, and other major metropolitan areas on Amtrak, commuter railroads, and freight railroads hosting passenger operations. Industry decision makers must frequently act on incomplete information. Therefore, more accurate, complete, and independently corroborated information leads to more sound decision-making. Railroads will err on the side of prudence and prefer to take more security actions than necessary to prevent or minimize possible loss of life and property.

In this case, government information sharing with critical infrastructure owners and operators in the rail sector lagged behind information from other sources (other sector ISACs and/or press reports) by between three and four hours with the notable exception of NYPD. In addition, the PT/ST-ISAC provided the initial reporting to other potentially affected sectors, the reports did not come from government officials. Based on subsequent interviews and discussions, the reasons for these delays vary. Sometimes government must corroborate information before confirming or denying it publicly. Because the public generally perceives the government to be the authoritative voice in these instances, some government officials believe they cannot retract a mistake made in public. This often delays officials from saying anything during a crisis. Sometimes classified information is "originator controlled," which makes it difficult to obtain the permissions needed to release it outside government-classified controls. It is common for private sector participants or members of the media to be on the scene before government officials.

Regarding NYPD, two strategic initiatives seem to have paid dividends in early warning: (1) two-way information sharing and (2) enhanced responsiveness. First, an NYPD detective detailed to London provided a direct link to ongoing analysis. This bi-directional communication conduit provided built-in advantages to both NYPD and to Scotland Yard. Second, APPL, NEXUS, and SHIELD programs provided for rapid notification of and dialog with New York private sector security directors. The value in these programs was in their pre-identification of trusted points of contact and establishment of redundant communications architectures in advance of the need.

Lessons learned from this case are that a pre-planned architecture for rapid information sharing between government and the private sector is essential to preparedness and that industry will not wait for confirmation from a government source before acting in its own (and the country's) defense. This reinforces the Study Group's findings regarding trusted relationships, robust information fusion capability, and expedited requests for information.

D. New York Public Transit Threat Alert, October 2005

Summary

On October 6, 2005, the NYPD increased security activities across its subway system based on evidence that terrorist leaders had deployed 19 operatives to New York to place bombs in the subway. The NYPD was acting on information allegedly obtained from one of three Iraqi insurgents arrested several days before, during a raid by a joint FBI-CIA team. According to two sources, the 19 operatives were to place improvised explosive devices in the subways using briefcases as cover. New York Mayor Michael Bloomberg and NYPD Police Commissioner Raymond Kelly held a press conference announcing that police would continue to check bags, briefcases, luggage, and strollers and additional uniformed and undercover officers would be riding in individual subway cars and present in stations throughout the system and commuter rail terminals.

Although Federal officials from DHS questioned the source's credibility, NYPD officials believed the threat was of enough substance to warrant the implementation of heightened security. New York officials cited their responsibility to protect New York and act with an

abundance of caution. Heightened security remained in place for three days before authorities could disprove the threat and completely discount the source. At that time, NYPD gradually reduced the additional security measures and returned to their normal level of elevated vigilance.

Timeline

Abbreviations used:

AAR	Association of American Railroads
APPL	NYPD Area Police/Private Security Liaison (communication mechanism between NYPD and New York City private security directors—primarily e-mail, with phone and physical meetings as backup)
JTTF	Joint Terrorism Task Force
NEXUS	NYPD program centering on personal contact with New York businesses, including information on "terrorist indicators" to watch for, literature, signage to post, and contact information
RAN	Railroad Alert Network
ST/PT-ISAC	Surface Transportation/Public Transportation Information Sharing and Analysis Center
TSA	Transportation Security Administration, U.S. Department of Homeland Security

Time (EDT)	Contact	Content
Wednesday, October 5, 2005		
not rec	JTTF New York Field Office	Relayed information to NYPD from intelligence reports being relayed from Iraq
not rec	APPL	Relayed information to members with caveat that threat had "not been fully corroborated"—also heightened NYPD counter-terrorism measures in subways
not rec	NEXUS	Focused on hardware and beauty supply stores selling household and industrial chemicals capable of weaponization
not rec	Classified source (non-DHS)	Document provides warning to AAR Ops Center, ST/PT-ISAC, and Amtrak regarding threat
1030	AAR Ops Center	Forwards Heightened Awareness (HA) bulletin issued by ST/PT-ISAC to Railroad Alert Network (RAN) for information and action
Thursday, October 6, 2005		
Morning	Classified source (non-DHS)	Classified bulletin sent to AAR Ops Center
Morning	AAR Ops Center	Relays information to Amtrak
1700	TSA Administrator	Secure telephone call with CEO, AAR (NYC press conference begins while call in progress)
1730	NY City Mayor Bloomberg, NYPD Commissioner Kelly, FBI	Press conference: Heightened threat "in the coming days"…"not corroborated" but worthy of action - asking the public to curtail their use of bags, suitcases, etc. for the short-term - stepped-up bag searches at this time. DHS did not raise the threat level for NYC (it remained at "Orange—High").

not rec	ST/PT-ISAC	Issued HA Update 1
not rec	ABC News	Report: "Police Investigate New York Subway Terror Threat"[18]
2300	DHS/FBI	Joint Bulletin received by AAR Ops
Friday, October 7, 2005		
0714	AAR Ops	Forwards DHS/FBI Joint Bulletin to RAN
not rec	Fox News	Report: "NYC Ups Subway Security After Bomb Threats"--New York subway could be the target of a terrorist attack in coming days. DHS officials in Washington downplayed the threat, saying it was of "doubtful credibility."[19]
Sunday, October 9, 2005		
0819	MSNBC (AP)	Report: "Authorities debate credibility of alleged NY plot"[20]

Conclusions

The scenario for this case was similar to the Financial Services alert case in the respect that intelligence analysis indicated a threat to a critical infrastructure sector in a specific location. However, in the year between these two cases, communication between government and this sector had improved dramatically. The study shows that government officials proactively shared information on the potential threat with NYPD and AAR before informing the public. Even though some analysts at the national level had serious doubts regarding the credibility of the information, they thought it prudent to provide advance warning to industry. The rail industry and NYPD executed appropriate protective actions, and maintained vigilance until Federal officials downgraded the threat.

The lesson: trusted relationships and existing information-sharing architectures work. This reinforces the Study Group's finding calling for establishing such relationships, and it demonstrates the usefulness of these relationships.

[18] http://abcnews.go.com/U.S./story?id=1190231
[19] http://www.foxnews.com/story/0,2933,171491,00.html
[20] http://www.msnbc.msn.com/id/9614242/

E. Overall Conclusions

In these four case studies, the goals of each of the stakeholders have been synonymous: prevent terrorist attacks on U.S. critical infrastructures or mitigate the effects of any that succeed. The problems identified pre-date DHS and they illustrate the objectives the department must have regarding information sharing. In this age of continuing terrorist threats to U.S. interests, the Federal government must engage the private sector early in analyzing and disseminating information and intelligence. Private sector expertise is critical in knowing what bits of information are important, knowing who to contact with the information, and knowing what action to take as a result.

To be clear, the lessons learned here are not limited to DHS. Indeed, the scope of this NIAC Intelligence Coordination study is national. The conclusions presented here provide strong anecdotal evidence, based on facts, to support the findings of the Study Group.

Findings

The Study Group developed four key findings. They are repeated here to allow readers to easily compare the findings to the case study conclusions.

1. **National-Level Fusion Capability:** A national-level fusion capability is required to gather, analyze, and disseminate information and intelligence relevant to CIP. This fusion capability must include the ability to manage requests for information to and from the private sector and government. It must also include the ability to merge information from intelligence agencies, law enforcement, and private sector expertise.

2. **Trusted Relationships:** Trusted relationships are vital to effective CIP. Key owners and operators need to develop relationships with key IC analysts. There is also a need to educate the IC analysts about critical infrastructure in the United States. Specifically, IC analysts need to understand how they operate, what they consider critical, and what kinds of information serve as "triggers" for response actions. The IC must have a way to leverage private sector expertise for better analysis as appropriate. Trusted relationships may depend more on process than individual relationships. Therefore there is a need for a structure that provides for this trusted environment.

3. **Request For Information Mechanism:** There is a need for a streamlined RFI mechanism that provides open and timely exchange of information between the IC and the private sector. Both sides in this partnership need to know how to ask key questions, to whom they need to direct these questions, and how to prioritize their responses.

4. **Information Protection:** There is a need for special information protection for sensitive critical infrastructure information shared between the IC and the private sector. This protection must be separate from the existing national security classification system, including caveats. All parties should protect information from disclosure, until disclosure is appropriate. This protection mechanism must be common across the private sector and the IC. It must been easy and timely for the private sector to utilize or it will cause

additional coordination problems. As an adjunct to this, there is also a need to improve dissemination of classified information to key private sector decision makers, as appropriate.

Case Study Acknowledgements

The Study Group would like to thank the following individuals and organizations for their outstanding support and contributions to this case study effort.

Peter Allor, *Information Technology Information Sharing and Analysis Center*
Suzanne Gorman, *Financial Services Information Sharing and Analysis Center*
Al Hancock, *Xcel Energy*
Patrick Kelleher, Dir, Worldwide Security, *Merrill Lynch*
Darren Lacey, CIO, *Johns Hopkins University/Johns Hopkins Medicine*
Lou Leffler, *North American Electric Reliability Council*
Lt. Paul Mauro, *New York Police Department*
Roger Platt, *Real Estate Information Sharing and Analysis Center*
Nancy Wilson, VP-Security, *Association of American Railroads*
G. Rick Wilson, *National Security Agency*
Ken Watson, *Cisco Systems, Inc*.

Appendix C– The Intelligence Community[21]

The IC is a federation consisting of members from Executive Branch agencies and organizations that work independently and jointly in an effort to conduct the intelligence activities necessary for foreign relations and national security. These activities include:

- collecting information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities;
- collecting information concerning, and the conduct of activities to protect against, intelligence activities directed against the U.S., international terrorist and international narcotics activities, and other hostile activities directed against the U.S. by foreign powers, organizations, persons, and their agents;
- producing and disseminating raw intelligence;
- analyzing all-source intelligence and the production and dissemination of finished intelligence to enable U.S. policymakers to better understand international political, economic, and military developments; and
- performing special activities, including authorized activities within the United States and abroad, as well as ad hoc intelligence activities directed by the President.

A. Members

An IC member works for a Federal government agency, service, bureau, or other organization within the Executive Branch that plays a role in the business of national intelligence. The IC comprises many such organizations. Except for the Central Intelligence Agency (CIA), intelligence offices or agencies are components of cabinet departments with other roles and missions. The intelligence offices/agencies, however, participate in IC activities and serve to support the other efforts of their departments.

The **Central Intelligence Agency (CIA)** has all-source analytical capabilities that cover the whole world outside U.S. borders. It produces a range of studies that cover virtually any topic of interest to national security policymakers. CIA also collects intelligence with human sources and, on occasion, undertakes covert actions at the direction of the President. (A covert action is an activity or activities of the U.S. Government to influence political, economic, or military conditions abroad, where the United States intends that its role will not be apparent or acknowledged publicly.)

Four major intelligence agencies in the Department of Defense (DoD) - the **National Security Agency (NSA)**, the **National Reconnaissance Office (NRO)**, the **National Geospatial-Intelligence Agency (NGA)**, and the **Defense Intelligence Agency (DIA)** - absorb the larger part of the national intelligence budget. NSA is responsible for signals intelligence and has collection sites throughout the world. The NRO develops and operates reconnaissance satellites. The NGA prepares the geospatial data - ranging from maps and charts to sophisticated

[21] www.intelligence.gov

computerized databases - necessary for targeting in an era dependent upon precision guided weapons. DIA is responsible for defense attaches and for providing DoD with a variety of intelligence products. Although the Intelligence Reform Act provides extensive budgetary and management authorities over these agencies to the Director of National Intelligence, it does not revoke the responsibilities of the Secretary of Defense for these agencies.

The **State Department's Bureau of Intelligence and Research (INR)** is one of the smaller components of the Intelligence Community but is widely recognized for the high quality of its analysis. INR is strictly an analytical agency; diplomatic reporting from embassies, though highly useful to intelligence analysts. Officials do not consider INR to be an intelligence function and they do not budget it as one.

The key intelligence functions of the **Federal Bureau of Investigation (FBI)** relate to counterterrorism and counterintelligence. The former mission has grown enormously in importance since September 2001, the bureau has hired many new analysts and officials have reorganized the FBI in an attempt to ensure that intelligence functions are not subordinated to traditional law enforcement efforts. Most importantly, the IC expects the FBI to forward law enforcement information to other intelligence agencies for use in all-source products.

The intelligence organizations of the four military services (**Air Force**, **Army**, **Navy**, and **Marines**) concentrate largely on concerns related to their specific missions. Their analytical products, along with those of DIA, supplement the work of CIA analysts and provide greater depth on key technical issues.

The Homeland Security Act provided the **Department of Homeland Security (DHS)** responsibilities for fusing law enforcement and intelligence information relating to terrorist threats to the homeland. The Information Analysis and Infrastructure Protection Directorate in DHS participates in the inter-agency counterterrorism efforts and, along with the FBI, has focused on ensuring that state and local law enforcement officials receive information on terrorist threats from national-level intelligence agencies.

The **Coast Guard**, now part of DHS, deals with information relating to maritime security and homeland defense.

The **Energy Department** analyzes foreign nuclear weapons programs as well as nuclear non-proliferation and energy-security issues. It also has a robust counterintelligence effort.

The **Department of the Treasury** collects and processes information that may affect U.S. fiscal and monetary policies. Treasury also covers the terrorist financing issue.

The **Drug Enforcement Administration** is the agency responsible for enforcing the controlled substances laws and regulations of the United States.

The **Office of the Director of National Intelligence** serves as the head of national intelligence (CI) for the U.S. Government and is directly responsible to the President.[22]

B. Intelligence Community Authorities

National Security Act of 1947[23]

The National Security Act of 1947 mandated a major reorganization of the foreign policy and military establishments of the U.S. Government. The act created many of the institutions that Presidents found useful when formulating and implementing foreign policy, including the National Security Council (NSC). The Council itself included the President, Vice President, Secretary of State, Secretary of Defense, and other members (such as the Director of the Central Intelligence Agency), who met at the White House to discuss both long-term problems and more immediate national security crises. A small NSC staff was hired to coordinate foreign policy materials from other agencies for the President. Beginning in 1953 the President's Assistant for National Security Affairs directed this staff. Each President has accorded the NSC with different degrees of importance and has given the NSC staff varying levels of autonomy and influence over other agencies such as the Departments of State and Defense. President Dwight D. Eisenhower, for example, used the NSC meetings to make key foreign policy decisions, while Presidents John F. Kennedy and Lyndon B. Johnson preferred to work more informally through trusted associates. Under President Richard M. Nixon, the NSC staff, then headed by Secretary of State Henry A. Kissinger, transformed itself from a coordinating body into an organization that actively engaged in negotiations with foreign leaders and implementing the President's decisions. The NSC meetings themselves, however, were infrequent and merely confirmed decisions already agreed upon by President Nixon and Secretary Kissinger.

The act also established the Central Intelligence Agency (CIA), which grew out of World War II era Office of Strategic Services and small post-war intelligence organizations. The CIA served as the primary civilian intelligence-gathering organization in the government. Later, the Defense Intelligence Agency became the main military intelligence body. The 1947 law also caused far-reaching changes in the military establishment. The War Department and Navy Department merged into a single Department of Defense under the Secretary of Defense, who also directed the newly created Department of the Air Force. However, each of the three branches maintained their own service secretaries. In 1949, Congress amended the act to give the Secretary of Defense more power over the individual services and their secretaries.

Executive Order 12333[24]

On December 4 1981, almost a year into his Administration, President Reagan issued his Executive Order on intelligence (E.O. 12333). It generally reaffirmed the functions of intelligence agencies (as outlined in the previous order) and continued most of the previous restrictions, but it set a more positive tone than its predecessor, and gave the CIA greater latitude to gather foreign intelligence within the United States and to provide assistance to law

[22] "Intelligence Reform and Terrorism Prevention Act of 2004," PL 108-408 §§ 7211-7214,. 118 Stat. 3638, 3825-3832, December 17, 2004

[23] http://www.milnet.com/1947-act.htm

[24] http://www.cia.gov/cia/information/eo12333.html (ref: Executive Order 12333 of Dec. 4, 1981, at 46 FR 59941, 3 CFR, 1981 Comp., p. 200ff)

enforcement. The Executive Order also provided a new NSC structure for reviewing intelligence activities, including covert actions.

EO 12333 has a short preamble and three parts:

Part 1. *Goals, Direction, Duties, and Responsibilities With Respect to the National Intelligence Effort*

- 1.1 Goals
- 1.2 The National Security Council
- 1.3 National Foreign Intelligence Advisory Groups
- 1.4 The Intelligence Community
- 1.5 Director of Central Intelligence
- 1.6 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies
- 1.7 Senior Officials of the Intelligence Community
- 1.8 The Central Intelligence Agency
- 1.9 The Department of State
- 1.10 The Department of the Treasury
- 1.11 The Department of Defense
- 1.12 Intelligence Components Utilized by the Secretary of Defense
- 1.13 The Department of Energy
- 1.14 The Federal Bureau of Investigation

Part 2. *Conduct of Intelligence Activities*

- 2.1 Need
- 2.2 Purpose
- 2.3 Collection of Information
- 2.4 Collection Techniques
- 2.5 Attorney General Approval
- 2.6 Assistance to Law Enforcement Authorities
- 2.7 Contracting
- 2.8 Consistency With Other Laws
- 2.9 Undisclosed Participation in Organizations Within the United States
- 2.10 Human Experimentation
- 2.11 Prohibition on Assassination
- 2.12 Indirect Participation

Part 3. *General Provisions*

- 3.1 Congressional Oversight
- 3.2 Implementation
- 3.3 Procedures
- 3.4 Definitions
- 3.5 Purpose and Effect
- 3.6 Revocation

Presidential Decision Directive (PDD) 35

Signed March 2, 1995, Presidential Decision Directive 35 (PDD-35) defines intelligence requirements from tier 0 to tier 4. Tier 0 is warning and crisis management. Tier 4 is countries

that are virtually of no interest to the United States. The PDD specifically identifies targets that the U.S. intelligence community will not collect against.

Under PDD-35, highest priority is assigned to intelligence Support to Military Operations [SMO]. The second priority is providing political, economic, and military intelligence on countries hostile to the United States to help to stop crises and conflicts before they start. The third priority is designed to protect Americans from new trans-national threats such as drug traffickers, terrorists, organized criminals, and weapons of mass destruction. PDD-35 also assigns high priority to Intelligence support to activities addressing counter-proliferation, as well as international terrorism, crime and drugs.

The Directive increased the priority assigned by the intelligence collection and analysis capabilities to the proliferation threat. In 1993, the Director of Central Intelligence established the Nonproliferation Center (NPC) to provide IC-level coordination for community nonproliferation programs. IC components are focusing on closing the knowledge gaps related to the proliferation activities of several countries.

This Directive established the Intelligence Priorities Interagency Working Group [IWG] as the forum for identifying foreign policy issues that are of sufficiently critical nature as to require amplified attention from the intelligence community. In addition, agencies represented in this interagency Working Group have established intelligence requirements groups to collect, analyze and rank strategic intelligence requirements and to represent these agency-level requirements at periodic meetings with the intelligence community to set intelligence requirements.

Guided by explicit intelligence priorities that the President established in PDD-35, the FY1997 intelligence budget request included realigned funds within national and tactical intelligence to satisfy the top PDD-35 priorities, such as support to military operations and counter-proliferation.[25]

Intelligence Reform and Terrorism Prevention Act of 2004

Published December 17, 2004, the Intelligence Reform and Terrorism Prevention Act 0f 2004 introduced the farthest-reaching reform in U.S. intelligence operations in decades. It called for a national intelligence director to oversee all intelligence agencies, and increased border patrol, port and aviation security.[26] The key provisions of this law:

- established the Director of National Intelligence, as it reorganized and improved the management of the IC, revised the definition of national intelligence, and established joint procedures for operational coordination between the Department of Defense and the CIA;
- established the National Counterterrorism Center, National Counter Proliferation Center, and National Intelligence Centers;
- established the Joint Intelligence Community Council

[25] http://www.fas.org/irp/offdocs/pdd35.htm
[26] http://www.cfr.org/publication/9110/

- made improvements in IC education;
- developed coordination processes for Service and national labs and the IC, open-source intelligence, and a National Intelligence Reserve Corps;
- established a Privacy and Civil Liberties Oversight Board; and
- identified other matters to improve the overall national intelligence effort.

National Intelligence Priorities Framework (NIPF)

The President signed National Security Presidential Directive 26 (NSPD-26) to create a dynamic process for articulating and reviewing intelligence priorities. Director of Central Intelligence Directive 2/3 established a National Intelligence Priorities Framework as a mechanism to translate the national foreign intelligence objectives and priorities approved by the National Security Council into specific guidance and resource allocations for the Intelligence Community.[27]

[The national] intelligence office has established a National Intelligence Priorities Framework, a three-tiered listing by importance of about 30 intelligence targets, signed by President Bush. …The top tier includes terrorism, weapons of mass destruction, Iraq, Iran, North Korea and China. (Testimony of Gen. Michael V. Hayden, Deputy Director of National Intelligence, April 14, 2006.)[28] Previous Presidents had similar priority lists.

[27] Tenet, George, Written Statement for the Record of the Director of Central Intelligence before the National Commission on Terrorist Attacks Upon the United States, March 24, 2004

[28] Pincus, Walter, "Intelligence Office Gives Progress Report," Washington Post, Friday, April 14, 2006; Page A11 (http://www.washingtonpost.com/wp-dyn/content/article/2006/04/13/AR2006041302040.html)

Appendix D – Critical Infrastructure Owners and Operators

The concept of "critical infrastructures" began with the President's Commission on Critical Infrastructure Protection (PCCIP), which produced its report in October 1997. The report defined eight sectors as critical to the nation. In 1998, Presidential Decision Directive 63 (PDD-63) embraced these same eight sectors and PDD-63 issued a call for Sector Coordinators and the establishment of Information Sharing and Analysis Centers (ISACs). Since then, Homeland Security Presidential Directive 7 (HSPD-7), the USA PATRIOT Act, and DHS have expanded and refined that list and clarified relationships between the public and private sectors for facilitating the protection of critical infrastructures.

> *Critical infrastructures are physical or virtual systems and assets or key resources so vital that their incapacity or destruction would have a debilitating impact on national economic security, public health or safety, or any combination of those matters.*[29]

Today, there are 17 defined CI/KR sectors, listed below:

- Communications
- Chemical and hazardous materials
- Commercial facilities
- Dams
- Defense industrial base
- Energy
- Emergency services
- Financial services
- Food and agriculture
- Government facilities
- Information technology
- National monuments and icons
- Nuclear power plants
- Postal and shipping
- Public health and healthcare
- Transportation
- Water

The single defining characteristic of these sectors is that they are diverse. Some sectors, such as the Nuclear sector, have a finite number of assets of similar characteristics while others include thousands of disparate sub-sectors, many of which cannot define physical perimeters or specific physical assets to protect. For example, the Food and Agriculture Sector Coordinating Council (FASCC) and its seven constituent sub-councils are comprised of 181 separate entities, representing millions of owners and operators "from farm to table," including grocery stores, restaurants, food processors, warehouses, agriculture inputs, and farms. Likewise, the Financial

[29] Public Law 107-56, USA PATRIOT Act, October 26, 2001, Section 1016.e

Services Sector Coordinating Council (FSSCC) is diverse, as well as international, and it includes brokerage firms, banks (which are regulated at the Federal level), and insurance companies (regulated by states). The electricity sector is "North American," not just U.S.-based, since it includes operations in Canada and Mexico. Railroads cover the United States, Canada, and northern Mexico. The IT and Communications sectors are international by nature, especially as they rely on the global Internet infrastructure.

Critical infrastructure owners and operators are in the business of providing essential services to customers, including governments, hospitals, first responders, citizens, and even each other. Most critical infrastructure organizations are suppliers, integrators, and users of one or more of the other infrastructure's services.

Each of the critical infrastructures is vital to the U.S. economy. The impact of outages in electricity or communications from a terrorist attack or major hurricane is immediate. While most Americans understand the dependency on those two sectors, most may not be as aware of America's dependence on railroads. Railroads transport 42 percent of intercity ton-miles, 64 percent of the coal used for electric power, 40 percent of America's grain harvest, 70 percent of the automobiles made in America, and 20 percent of the chemicals used in the nation—even more of those essential to public health. Chlorine is used in 98 percent of all water treatment, 85 percent of pharmaceuticals, and 96 percent of crop protection. Trucks cannot pick up the slack, since only 82 nationwide can haul over 20 tons of chlorine.[30] Railroads also represent a vital link in multi-modal shipping, working closely with maritime shipping and the trucking industry.

Most owners and operators understand the impact on national and economic security of their decisions regarding security and business continuity. Most responded expeditiously to government requests that they self-organize SCCs and ISACs, if appropriate, to facilitate public-private information sharing and coordination. Indeed, the FSSCC predates DHS, as does the communications sector's National Coordinating Center (NCC).

ISACs coordinate day-to-day information and analysis on threats, vulnerabilities, countermeasures, and best practices that apply to their sectors. Cross-ISAC information sharing has also proven to be valuable to critical infrastructure owners and operators. The leadership of 11 ISACs formed the ISAC Council to strengthen cross-sector operational information sharing and assist each ISAC to take advantage of best practices developed by the others.

Established in 2000, the PCIS coordinates cross-sector initiatives to promote assured and reliable provision of critical infrastructure services in the face of emerging risks to economic and national security. PCIS members are representatives of the SCCs. Whereas the ISACs coordinate and disseminate *operational-level* information, the SCCs and PCIS coordinate, in concert with DHS, SSAs, and GCCs, *policy and strategic* issues for the critical infrastructures.

The Critical Infrastructure Partnership Advisory Council (CIPAC), which the DHS Secretary implemented on March 21, 2006[31], facilitates regular, ongoing, multi-directional communication and coordination between CI/KR owners and operators and government. It also provides policy

[30] Cross-Sector Interdependencies and Risk Assessment Guidance, NIAC, January 13, 2004

[31] Federal Register / Vol. 71, No. 57 / Friday, March 24, 2006

advice as it emerges from those discussions. CIPAC members comprise both private sector and government stakeholders:

- CI/KR owners and operators that are members of their respective sector's recognized SCC, including their representative trade or equivalent organizations; and
- Federal, State, local, and tribal governmental entities comprising the members of the GCC for each sector, including their representative trade or equivalent organizations.

In effect, CIPAC is an umbrella framework to facilitate trusted bi-directional information flow between the PCIS and SCCs and their government counterparts. As these entities engage more and more under this framework, CIPAC should prove to be a valuable forum for government and private sector critical infrastructure stakeholders.

Appendix E – Information Sharing

Information sharing is vital for protecting the nation's CI/KR, yet views and definitions of this function vary widely. Since DHS' inception, strategies for infrastructure protection have evolved, and the aims and scope of information sharing have expanded. Gone are the days when Federal officials limited information sharing to the communication of specific threats, incidents, alerts, and warnings concerning our critical infrastructure.

The Information Sharing Landscape

Information sharing covers a myriad of bi-directional information exchanges between the private sector and state, local, and Federal government. It involves a wide variety of participants including law enforcement, CEOs, corporate security officers, sector-specific associations, and the Intelligence Community. The goals of information sharing also differ across the spectrum of Homeland Security, as indicated above, from proactive risk management and long-term, strategic planning to reactive, pre-incident, near-term deterrence and protection, and to post-incident response and recovery.

Information to be shared falls into three primary categories: (1) strategic threat information that drives investment and expenditures; (2) situational awareness information around assets and systems on a daily basis, including notification that nothing is threatening; and (3) alerts and warnings of a potential imminent threat.

Deterring attack has generally fallen to law enforcement and to the government, whose objective is to reduce the threats and threat capabilities of the nation's enemies. Owners and operators may contribute to deterrence by noting and reporting anomalous activities around their business operations. However, infrastructure owners and operators also discourage potential threats when they take steps to make their structures and processes difficult or unattractive targets for potential perpetrators.

Protection actions include reducing vulnerabilities and diminishing the significance of individual assets or systems to an infrastructure's overall operation. As part of long-term planning, critical infrastructure owners and operators sometimes need threat information from the government and might want to participate with the government in risk and vulnerability assessment. The types of information the private sector needs for planning purposes include terrorist modus operandi and threat trends, especially vis-à-vis specific geographical regions or specific critical infrastructure.

Preparedness actions include planning and implementation of programs to enhance readiness, which includes vulnerability reduction investments, identification of resources at risk, training, and implementation of business continuity plans.

Crisis management and ***response*** is intended to reduce damage to the greatest extent possible during an incident and to facilitate ***recovery (restoration*** and ***reconstitution)*** as quickly as possible. Effective response and recovery plans are the means by which officials manage residual risk after whatever risk reduction they have accomplished through deterrence and protection.

Owners and operators will generally accept a risk of possible disruption if they do not have sufficient information to prioritize investments in preparedness, particularly protection activities such as vulnerability reduction. If an organization does not invest in deterrence, or protection against a particular threat, by default it then accepts the costs of response and recovery of its business operations as its primary risk management action. If it does not have business continuity plans in place to respond and recover, then it also accepts the greater risk of experiencing financial setbacks or going out of business. Relevant information is an important determinant of appropriate levels of investments over the range of possible risk management actions. **The more specific and relevant the information available, the more likely the critical infrastructure entity will invest in preparedness, deterrence and protective actions such as vulnerability reduction actions.**

Meaningful, actionable information (as defined by the CI/KR owners and operators) is also essential for effective execution of risk management (tactical) actions. This information is apt to be different in form and content from the information owners and operators need to make strategic policy and investment decisions. Owners and operators' primary focus, by definition, is running their business operations on a daily basis. Threat and warning information represent the trigger by which they take immediate action to protect their operations.

Information Sharing and Intelligence Coordination

Information that the government shares with the private sector is specific information that may be sensitive or classified information collected, analyzed, and developed into intelligence products by the IC. Even when the private sector provides information to Federal, State, local or tribal agencies, the government agency may fuse the information with additional information from the IC. The result of this fusion is an intelligence product. Furthermore, the information may pertain to national risks and vulnerabilities in CIP, whether classified or not, and as such, protecting the information is also part of protecting the infrastructure. This intelligence coordination presents a unique set of problems, with the burden of responsibility on the IC to sort out whether the government can and should share the information with the private sector.

Existing Mechanisms for Information Sharing

DHS, working closely with the private sector, has already begun to implement a number of mechanisms for information sharing. These include all the Homeland Security Information Network (HSIN) variants, the Executive Notification System (ENS), the CIPAC, the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), the National Infrastructure Coordinating Center (NICC), and the PCII office and program.

The consensus of the Council is that multiple complementary mechanisms are in place now, but for them to succeed it will require formal documentation, explanation, and training within the government and with private sector partners.

CIPAC membership encompasses CI/KR owner/operator institutions and their designated trade or equivalent organizations that are identified as members of existing SCCs. The membership also includes representatives from Federal, State, local, and tribal governmental entities identified as members of existing GCCs for each sector.

Officials should study whether HITRAC could serve as an appropriate vehicle for a national intelligence fusion capability. DHS may improve existing mechanisms by inclusion of additional private sector expertise—most likely as part of HITRAC—and by addressing some of the obstacles that these mechanisms face.

Appendix F – Glossary

Business Continuity – The ability of an organization to continue to function before, during and after a disaster

Catastrophic Incident - Any natural or manmade incident including terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. A catastrophic event could result in sustained national impacts over a prolonged period; almost immediately exceeds resources normally available to State, local, tribal, and private sector authorities in the impacted area; and significantly interrupts governmental operations and emergency services to such an extent that national security could be threatened. All catastrophic events are Incidents of National Significance.

CIFA – Department of Defense Counterintelligence Field Activity

Common Operating Picture (COP) - A broad view of an overall situation as reflected by situation reports, aerial photography, and other information or intelligence.

Confidential – In terms of U.S. classified information markings, "Confidential" shall be applied to information where unauthorized disclosure could be reasonably expected to cause damage to the national security.

Consequence – The result of a terrorist attack on infrastructure assets reflecting the level, duration, and nature of the loss resulting from the attack. HSPD 7 notes three types of consequences:

> **Exploitation:** the use of an infrastructure asset against some other target. Any evaluation of the consequences of the exploitation of an asset must consider whether the asset can be modified, influenced, changed, employed, leveraged, or commandeered in a manner that would enable attacks on other targets.
> **Destruction:** the total loss of an infrastructure asset, function, or service; a permanent or long-term consequence. Destruction of an asset may also include collateral damage affecting related assets.
> **Incapacitation:** The partial loss of an infrastructure asset function, or service; a short-term consequence from which recovery is possible.

Counterintelligence - Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.

Credible Threat - A potential terrorist threat that, based on a threat assessment, is credible and likely to involve weapons of mass destruction (WMD).

Crisis Management – The identification, acquisition, and planning for resources needed to anticipate, prevent, and/or resolve a threat (natural or man-made) or act of terrorism.

Critical Infrastructures - Thirteen sectors that produce essential goods and services, provide interconnectedness and operability, account for public safety, and provide security vital to a strong national defense and thriving economy. The 13 identified sectors are:

- Food & Agriculture
- Banking & Finance
- Chemical & Hazardous Materials
- Defense Industrial Base
- Water
- Public Health
- Energy
- Emergency Services
- Information Technology
- Telecommunications
- Postal & Shipping
- Transportation

Critical Infrastructure Information (CII) - is defined as information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

> (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including misuse of or unauthorized access to all types of communications and data transmission systems), which violates Federal, State, or local law, harms interstate commerce, or threatens public health and safety;
>
> (B) the ability of critical infrastructure or protected systems to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or,
>
> (C) any planned or past operational problem or solution regarding critical infrastructure...including repair, recovery, reconstruction, insurance, or continuity to the extent it relates to such interference, compromise, or incapacitation.

Critical Infrastructure Protection – The activities undertaken through a risk management methodology that reduce risk for CI/KR assets or systems.

Cyber - Pertaining to computers and their computer networks.

Director of National Intelligence (DNI) - The Director of National Intelligence (DNI) serves as the head of the Intelligence Community (IC). The DNI also acts as the principal advisor to the President; the National Security Council, and the Homeland Security Council for intelligence matters related to the national security; and oversees and directs the implementation of the National Intelligence Program.

Domestic Intelligence, Domestic Intelligence Collection – Referenced in the 9/11 Commission report, domestic intelligence refers to threat information collected in the United States on U.S. organizations and U.S. persons.

Domestic terrorism - The Federal government defines domestic terrorism activities as those that **(A)** involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; **(B)** appear to be intended to:

(1) intimidate or coerce a civilian population;

(2) influence the policy of a government by intimidation or coercion; or

(3) affect the conduct of a government by mass destruction, assassination, or kidnapping.

and **(C)** occur primarily within the territorial jurisdiction of the United States (from the USA Patriot Act).

Deterrence - The act or process of discouraging actions or preventing occurrences by instilling fear or doubt or anxiety

Electronic surveillance - The acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication

Emergency - As defined by the Stafford Act, an emergency is "any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States."

Emergency Operations Center (EOC) - The physical location at which the coordination of information and resources to support domestic incident management activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire, law enforcement, and medical services), by jurisdiction (e.g., Federal, State, regional, county, city, tribal), or by some combination thereof.

Emergency Response Provider - Includes Federal, State, local, and tribal emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities

Federal - Of or pertaining to the Federal Government of the United States of America

Federal Advisory Council Act - In 1972, the Federal Advisory Committee Act (Public Law 92-463, 5 U.S.C., App) was enacted by Congress. Its purpose was to ensure that advice rendered to the executive branch by the various advisory committees, task forces, boards, and commissions formed over the years by Congress and the president, be both objective and accessible to the public. The Act not only formalized a process for establishing, operating, overseeing, and terminating these advisory bodies, but also created the Committee Management Secretariat

(MCC), an organization whose task it is to monitor and report executive branch compliance with the Act.

First Responder - Local and nongovernmental police, fire, and emergency personnel who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) who provide immediate support services during prevention, response, and recovery operations. First responders may include personnel from Federal, State, local, tribal, or nongovernmental organizations.

Foreign intelligence - Information relating to the capabilities, intentions and activities of foreign powers, organizations or persons.

For Official Use Only (FOUO) – Used by the Federal government, For Official Use Only (FOUO) is a document designation, not a national security classification. This designation is used by Department of Defense and a number of other federal agencies to identify information or material, which, although unclassified, may not be appropriate for public release. There is no national policy governing use of the For Official Use Only designation - **each agency is responsible for determining how it shall be used. The categories of protected information may be quite different from one agency to another, although in every case the protected information must be covered by one of the nine categories of information that are** *exempt from public release under FOIA***.**

Freedom of Information Act (FOIA) - The Freedom of Information Act of 1966 protects the rights of the public to information and makes provisions for individuals to obtain information on the operation of federal agencies.

Fusion Center – An organized structure to coalesce data and information for the purpose of analyzing, linking and disseminating intelligence (information). Fused data are then analyzed to generate intelligence products and summaries for tactical, operational, and strategic commanders.

Government Coordination Council (GCC) - The government counterpart to the Sector Coordinating Council (SCC) for each sector, established to enable interagency coordination. The GCC is comprised of representatives across various levels of government (Federal, State, Territorial, local, and tribal) as appropriate to the security landscape of each individual sector.

The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) – Serves as the national center for the integration, analysis and sharing of information regarding the risks of terrorist attacks to U.S. infrastructure for stakeholders within DHS, other Federal departments and agencies, the Intelligence Community, state and local governments and law enforcement agencies, and in the private sector.

Homeland Security - A concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.

Homeland Security Advisory Council (HSAC) - The Homeland Security Advisory Council (HSAC) provides advice and recommendations to the Secretary on matters related to homeland security. The Council is comprised of leaders from state and local government, first responder communities, the private sector, and academia.

Homeland Security Information - 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.

Homeland Security Information Network - Critical Infrastructure (HSIN-CI) - Designed to communicate real-time information to critical infrastructure owners and operators – 80 percent of whom are part of the private sector.

Homeland Security Information Network – Critical Sectors (HSIN-CS) – Provides tools to facilitate information sharing.

Homeland Security Presidential Directive (HSPD-7) - This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

Incident of National Significance - Based on criteria established in HSPD-5 (paragraph 4), an actual or potential high-impact event that requires a coordinated and effective response by and appropriate combination of Federal, State, local, tribal, nongovernmental, and/or private sector entities in order to save lives and minimize damage, and provide the basis for long-term recovery.

Information Sharing and Analysis Center (ISAC) - Presidential Decision Directive (PDD)-63 established the concept of an Information Sharing and Analysis Center (ISAC) that would be a private sector entity responsible for gathering, analyzing, sanitizing, and disseminating to industry information related to vulnerabilities, threats, intrusions, and anomalies affecting the critical infrastructures.

Infrastructure - The manmade physical systems, assets, projects, and structures, publicly and/or privately owned, that are used by or provide benefit to the public. Examples of infrastructure include utilities, bridges, levees, drinking water systems, electrical systems, communications systems, dams, sewage systems, and roads.

Intelligence – The product of adding value to information and data through analysis. It is the process by which analysis is applied to information and data to inform policy-making, decision-making, including decisions regarding the allocation of resources, strategic decisions, operations and tactical decisions. Intelligence serves many purposes among which are the identification and elimination of threat sources, the investigation and resolution of threats, the identification and treatment of security risk, the elimination of threat sources, the mitigation of harm associated with risk, preemption, response, preparation and operations related to threats and risks.

Intelligence Community (IC) - A federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States. Members are:

- Office of the Director of National Intelligence
- Air Force Intelligence
- Army Intelligence
- Central Intelligence Agency
- Coast Guard Intelligence
- Defense Intelligence Agency
- Department of Energy
- Department of Homeland Security
- Department of State
- Department of the Treasury
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Marine Corps Intelligence
- National Geospatial-Intelligence Agency
- National Reconnaissance Office
- National Security Agency
- Navy Intelligence

Intelligence Coordination Study Group – Subject-matter experts from the critical infrastructure sectors and the Intelligence Community.

Intelligence Coordination Working Group – Members of the National Infrastructure Assurance Council (NIAC) who contributed to this effort to look at ways the Intelligence Community and the critical private sectors can work more effectively together.

Intelligence Cycle - The process by which information and data is collected, evaluated, stored, analyzed, and then produced for dissemination to the intelligence consumer.

Interdependency – The multi- or bi-directional reliance of an asset, system, network, or collection thereof, within of across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Key Resources (KR) – Facilities, sites, and groups of organized people, including:

- Dams;
- Government facilities;
- Commercial facilities; and
- Nuclear power plants;

whose destruction could cause large-scale injury, death, or destruction of property and/or profoundly damage our national prestige and confidence

Law Enforcement – Federal, State, local, and tribal agencies assigned to enforce the law. Law enforcement officials are often involved in collecting threat information.

Mitigation - Activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident.

Mobilization - The process and procedures used by all organizations—Federal, State, local, and tribal—for activating, assembling, and transporting all resources that have been requested to respond to or support an incident.

Multi-jurisdictional Incident - An incident requiring action from multiple agencies in which each has jurisdiction to manage certain aspects of the incident.

National - Of a nationwide character, including the Federal, State, local, and tribal aspects of governance and policy.

National Counterterrorism Center (NCTC) - The NCTC serves as the primary Federal organization for analyzing and integrating all intelligence possessed or acquired by the U.S. Government pertaining to terrorism and counterterrorism, excepting purely domestic counterterrorism information. The NCTC may, consistent with applicable law, receive, retain, and disseminate information from any Federal, State, or local government or other source necessary to fulfill its responsibilities.

National Foreign Intelligence Program - Includes the programs listed below, but its composition shall be subject to review by the National Security Council and modification by the President: (1) The programs of the CIA; (2) The Consolidated Cryptologic Program, the General Defense Intelligence Program, and the programs of the offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance, except such elements as the Director of Central Intelligence and the Secretary of Defense agree should be excluded; (3) Other programs of agencies within the Intelligence Community designated jointly by the Director of Central Intelligence and the head of the department or by the President as national foreign intelligence or counterintelligence activities; (4) Activities of the staff elements of the Director of Central Intelligence; (5) Activities to acquire the intelligence required for the planning and conduct of tactical operations by the United States military forces are not included in the National Foreign Intelligence Program.

National Infrastructure Assurance Council (NIAC) - Provides advice to the Secretary of Homeland Security and the President on the security of information systems for the public and

private institutions that constitute the critical infrastructure of our Nation's economy. This includes information systems in banking and finance, manufacturing and transportation, and emergency government information systems. The council is composed of a maximum of 30 members, appointed by the President from private industry, academia, and state and local government.

National Infrastructure Coordinating Center (NICC) - Managed by the DHS Information Analysis and Infrastructure Protection Directorate, the NICC monitors the Nation's critical infrastructures and key resources on an ongoing basis. In the event of an incident, the NICC provides a coordinating vehicle to share information with critical infrastructure and key resources information-sharing entities.

National Geospatial-Intelligence Agency (NGA) - Provides timely, relevant, and accurate geospatial intelligence in support of national security objectives. Geospatial intelligence is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth.

National Response Center - A national communications center for activities related to oil and hazardous substance response actions. The National Response Center, located at DHS/USCG Headquarters in Washington, DC, receives and relays notices of oil and hazardous substances releases to the appropriate Federal OSC.

Non-Disclosure Agreement (NDA) - A contract whereby one promises to treat information confidentially and not give out information without proper authorization.

Open source – Information and intelligence derived from publicly available sources.

Originator Control (ORCON) – A U.S. government distribution control for information and intelligence that means that any additional distribution or inclusion in another document must be approved by the originator of the document. It is used on intelligence information that could permit identification of a sensitive intelligence source or method.

Owners/Operators - Those entities responsible for day-to-day operation and investment in a critical infrastructure asset or system.

Preparedness - The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources.

Prevention - Actions taken to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions taken to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations;

investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine.

Protected Critical Infrastructure Information (PCII) Program - The PCII Program is designed to encourage private industry to share their sensitive and proprietary business information with the Federal Government on a voluntary basis. The Department of Homeland Security will use PCII in pursuit of a more secure homeland, focusing primarily on:

- Analyzing and securing critical infrastructure and protected systems,
- Identifying vulnerabilities and developing risk assessments, and
- Enhancing recovery preparedness measures.

Information submitted, if it satisfies the requirements of the Critical Infrastructure Information Act of 2002, is protected from public disclosure under:

- The Freedom of Information Act,
- State and local sunshine laws, and
- Use in civil litigation.

Prioritization – In the context of the NIPP, prioritization is the process of using risk assessment results to identify where risk-reduction or management efforts are most needed and subsequently determine which protective actions should be instituted in order to have the greatest effect

Private Sector - Organizations and entities that are not part of any governmental structure, including for-profit and not-for-profit organizations, formal and informal structures, commerce and industry, private emergency response organizations, and private voluntary organizations.

Proprietary - Owned by a private individual or corporation under a trademark or patent.

Protection – In the context of the NIPP, protection includes the activities that identify critical infrastructures and key resources (CI/KR), assess vulnerabilities, prioritize CI/KR, and develop protective programs and measures.

Raw intelligence - Unevaluated intelligence reporting, usually from a single source.

Recovery – In the context of the NIPP, it is the development, coordination, and execution of service- and site-restoration plans for impacted communities and the reconstitution of government operations and services through individual, private sector, nongovernmental, and public assistance programs that: identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as feasible; evaluate the incident to identify lessons learned; and develop initiatives to mitigate the effects of future incidents.

Request For Information (RFI) – A mutual and bi-directional processes for requesting information between the IC and the private sectors; prioritizing, vetting, and tracking information

requests; and reporting required information. An effective RFI process must address differences in vocabulary, provide for rapid feedback and response to requests, and ensure dissemination across the communities within obligations to protect information.

Residual Risk - Portion of risk remaining after security measures and mitigations have been applied.

Response – In the context of the NIPP, activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include: applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk – A measure of potential harm that encompasses threat, vulnerability, and consequence.

Risk Management Framework – A planning methodology that outlines the process for setting security goals; identifying assets, systems, networks, and functions; assessing risks; prioritizing and implementing protective programs; measuring performance; and taking corrective action.

Secret - In terms of U.S. classified information markings, "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

Sector Coordinating Council (SCC)- The private sector counterpart to the Government Coordinating Councils (GCCs), these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. SCCs serve as the government’s principal point of entry into each sector for developing and coordinating a wide range of CI/KR protection activities and issues.

Sector Partnership Model – The framework use to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for CI/KR protection involving all levels of government and private sector owner and operators.

Sector Specific Agency (SSA) – Federal departments and agencies identified under HSPD-7 as responsible for the protection activities in specified CI/KR sectors.

Sensitive But Unclassified (SBU) – Federal government label that refers to information that warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the Freedom of Information Act.

Sensitive Information – Any information that requires additional protection and more careful dissemination. Such information should be marked or labeled to indicate its special handling needs.

Situation Assessment - The evaluation and interpretation of information gathered from a variety of sources (including weather information and forecasts, computerized models, GIS data mapping, remote sensing sources, ground surveys, etc.) that, when communicated to emergency managers and decision makers, can provide a basis for incident management decision making.

Strategic – In the context of incident management, strategic elements are characterized by continuous, long-term, high-level planning by organizations headed by elected or other senior officials. These elements involve the adoption of long-range goals and objectives, the setting of priorities, the establishment of budgets and other fiscal decisions, policy development, and the application of measures of performance or effectiveness.

Subject-Matter Expert (SME) – An individual who is a technical expert in a specific area or in performing a specialized job, task, or skill.

Tear Line - the demarcation on an intelligence report (usually denoted by a series of dashes) where sanitized or less classified versions of the intelligence are presented. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with the "need-to-know" principle and other disclosure guidelines of the information below the tear line.

Telecommunications - The transmission, emission, or reception of voice and/or data through any medium by wire, radio, other electrical electromagnetic, or optical means. Telecommunications includes all aspects of transmitting information.

Terrorism - Any activity that (1) involves an act that (a) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and (b) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and (2) appears to be intended (a) to intimidate or coerce a civilian population; (b) to influence the policy of a government by intimidation or coercion; or (c) to affect the conduct of a government by mass destruction, assassination, or kidnapping.

Terrorism Information - all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to— (A) 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; (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (C) communications of or by such groups or individuals; or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Threat - An indication of possible violence, harm, or danger

Threshold of Criticality – A metric to assess importance and risk. Some systems/processes are critical taken together – i.e. the result of several repeated executions of the same process is critical to an organization, while a single execution of the process is of low consequence. These processes are said to have a *high* threshold of criticality. In contrast, there are processes where even a single execution of the process has significant risk and/or opportunity cost implications for the organization. Such processes have a *low* threshold of criticality. Processes with a high threshold of criticality typically represent lower risk, while processes or systems with a low threshold of criticality represent higher risk.

Top Secret - In terms of U.S. classified information markings, "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

Unclassified - Information that has not been determined to require protection against unauthorized disclosure and that is not designated as classified, pursuant to Executive Order 12958 or any predecessor order.

Vetting - To subject to thorough examination or evaluation, particularly applicable to review of personnel for positions of trust.

Vulnerability – A weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by an adversary, or disrupted by a natural hazard, or technological failure.

Weapon of Mass Destruction (WMD) - As defined in Title 18, U.S.C. § 2332a: (1) any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than 4 ounces, or missile having an explosive or incendiary charge of more than one-quarter ounce, or mine or similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

Appendix G -- References

Cumming, Alfred, and Todd Masse. Intelligence Reform Implementation at the Federal Bureau of Investigation: Issues and Options for Congress. Congressional Research Service: August 16, 2005. Online. Order Code RL33033.

Moteff, John D. Critical Infrastructures: Background, Policy, and Implementation. Congressional Research Service: July 12, 2005. Online. Order Code RL30153

New York Police Department. Operation Nexus: Fifth edition. New York: November 2005.

Reese, Shawn. Risk-Based Funding in Homeland Security Grant Legislation: Analysis of Issues for the 109th Congress. Congressional Research Service: August 29, 2005. Online. Order Code RL33050.

U.S. House of Representatives. Intelligence Reform and Terrorism Prevention Act of 2004: 108-796. December 7, 2004

U. S. Office of the Director of National Intelligence. The National Intelligence Strategy of the United States of America. Washington: October 2005.

U.S. Department of Homeland Security Science and Technology Directorate. Progress Report on the Department of Homeland Security's Risk Assessment Policy Group, Report to Congress in Response to the House Committee on Appropriations Report (H.REPT. 109-79) (Draft). Washington: January 2006.

U.S. Department of Homeland Security Information Analysis and Infrastructure Protection Directorate, Infrastructure Coordination Division. Report to Congress Critical Infrastructure and Key Resource Sector Information Sharing and Analysis Centers: Status. Washington: January 20, 2005.

U.S. Department of Homeland Security. Defense Industrial Base Sector Criticality Methodology. Washington: 2005.

U.S. Department of Homeland Security. Homeland Infrastructure Threat & Risk Analysis Center Presentation. Washington: 2005.

U.S. Department of Homeland Security. National Infrastructure Protection Plan Base Plan, Version 1. Washington: November 2, 2005.

U.S. Department of Homeland Security. Status of Information Sharing and Analysis Centers. Washington: 2005

U.S. President's Homeland Security Advisory Council. Private Sector Information Sharing Task Force on Homeland Security Information Sharing Between Government and the Private Sector. Washington: August 10, 2005.

Walker, David M. Comptroller General of the U.S. Testimony Before the Subcommittee on Management, Integration, and Oversight, Committee on Homeland Security, House of Representatives. Strategic Budgeting. Risk Management Principles Can Help DHS Allocate Resources to Highest Priorities. U.S. Government Accountability Office. Washington: June 29, 2005.

Watson, Ken. National Infrastructure Advisory Council Intelligence Coordination Study Group. Critical Infrastructure Protection: Intelligence Community Involvement. Washington: March 2005.

Willis, Henry, Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Kelly. Estimating Terrorism Risk. Rand Corporation, Arlington, VA: 2005.

Wilson, Colleen. U.S. Department of Homeland Security Information Sharing and Collaborative Office. Intelligence Community Information Sharing. Washington: August 2005.

Wong, Nancy J. Information Sharing and Analysis: Describing the Landscape for Private Sector. Washington: July 25, 2003.

Risk Assessment Policy Group, Lexicon Working Group, Draft Risk Lexicon-Version 1; January 2005.