National Infrastructure Advisory Council (NIAC)

Intelligence Information Sharing

January 10, 2012

Alfred R. Berkeley III
Chairman,
Pipeline Trading Systems LLC

Philip G. Heasley
President and CEO,
ACI Worldwide

James B. Nicholson
President and CEO,
PVS Chemicals, Inc.

James A. Reid
President,
CBRE Group, LLC
Eastern Division

Michael J. Wallace
Former Vice Chairman & COO,
Constellation Energy

Wesley Bush
Chairman, President & CEO
Northrop Grumman

Overview

- Study Leadership
- Charge to the Council
- Background
- Study Approach
- Findings and Recommendations
- Discussion and Questions

NIAC Working Group

- **Al Berkeley**, Chairman, Pipeline Trading Systems*
- **Phil Heasley**, President & CEO, ACI Worldwide*
- **Jim Nicholson**, President & CEO, PVS Chemicals*
- **Wes Bush**, Chairman, President & CEO, Northrop Grumman
- **Jim Reid**, President, CBRE Group, LLC – Eastern Division
- **Mike Wallace**, Former Vice Chairman & COO, Constellation Energy

** Co-Chairs*

NIAC Study Group

- **Joan Gehrke**, PVS Chemicals, Inc. **(Co-Chair)**
- **Robin Holliday**, Johns Hopkins University Applied Physics Laboratory **(Co-Chair)**
- **Gerald Buckwalter**, Northrop Grumman
- **Dr. Antonio DeSimone**, Johns Hopkins University Applied Physics Laboratory
- **Joseph Donovan**, Beacon Capital Partners, LLC
- **Dr. John Gannon**, BAE Systems
- **Ed Goetz**, Constellation Energy
- **Jay Montgomery**, Kinder Morgan
- **Dr. Erin Mullen**, PhRMA
- **Bill Muston**, Oncor Electric Deliver Company, LLC
- **Nitin Natarajan**, HHS/ASPR/OPEO
- **Raymond Reese**, Colonial Pipeline
- **Jim Rosenbluth**, Cushman & Wakefield, Inc.
- **Tim Scott**, Dow Chemical
- **Stan Szemborski**, Northrop Grumman

Charge to the Council

The Administration requested that the NIAC examine three aspects of intelligence information sharing:

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

* The Working Group interpreted "counterintelligence" to mean "counterterrorism."

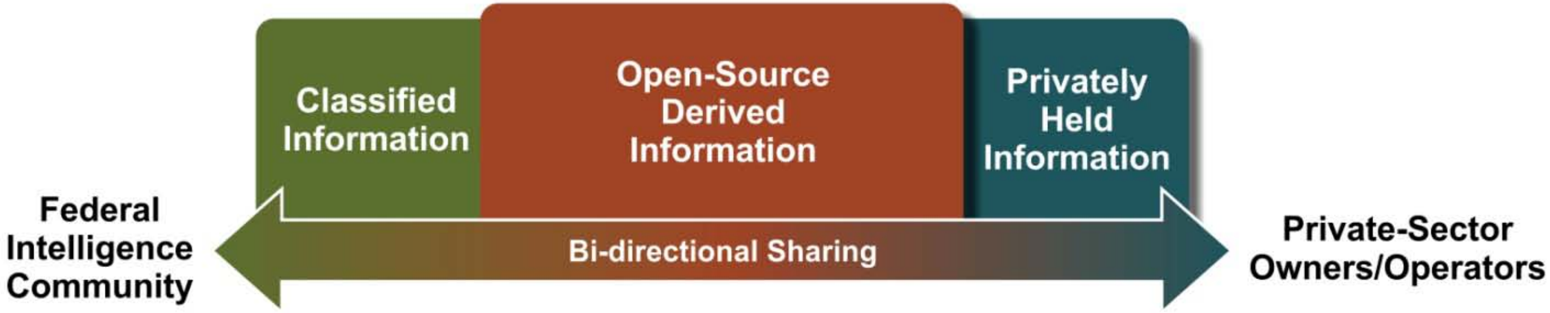
Background

- The Council's 2006 report on *Public-Private Sector Intelligence Coordination* recommended the development of bi-directional, sector-specific processes for sharing intelligence information with the private sector.

- At the April 13, 2010 NIAC Quarterly Business Meeting, DHS requested that the Council conduct an updated study on intelligence information sharing.

- The Council approved the study approach at the October 19, 2010 Quarterly Business Meeting.

Bi-directional Information Sharing


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

- The private sector is a relatively new partner and customer of the Federal Intelligence Community
- The private sector and the Federal Intelligence Community share the goal of risk reduction but have different purposes, incentives and rewards for sharing information
- Non-classified information held by the private sector can contribute to our understanding of national threats
- Open-source information and analysis is a growing portion of the flow of threat information
- Sharing classified information with the private sector is challenging
- Trusted organizational, functional, and personal relationships are important and must be developed and tested

Study Approach

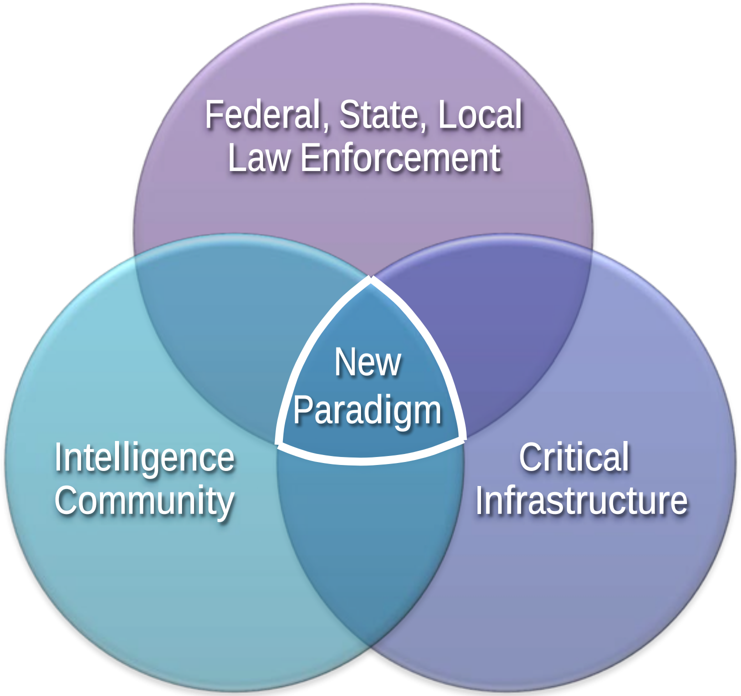
- Examined all stages of the intelligence cycle pertaining to public-private information sharing: requirements generation, information collection, analysis, and dissemination
- 200$^+$ interviews with security directors, senior executives, subject matter experts, government executives, and managers
- Comprehensive review of 255 open-source documents
- Detailed case studies of five critical infrastructure sectors to understand how sector characteristics shape information sharing needs

Sector Case Studies

- Banking and Financial Services Sector
- Chemical Sector
- Commercial Facilities Sector
- Energy Sector (Oil and Natural Gas)
- Healthcare and Public Health Sector

A Vision for Effective Intelligence Information Sharing

- Critical infrastructure (CI) owners and operators are a valued and trusted partner of the Intelligence Community.
- Collaboration among the Intelligence Community, law enforcement, and CI owners and operators is the new paradigm for effective intelligence sharing.
- The information requirements of the CI owners and operators are understood by the Intelligence Community.
- Intelligence information sharing is an integral part of public-private information sharing structures and processes.
- The capabilities of the CI owners and operators are understood and integrated into a *national* capability for intelligence information.



Foundation 1

1. **Important advances in intelligence sharing have been made in the past five years.**

   A. The Federal Intelligence Community, through the leadership of the Director of National Intelligence, appears to have improved information sharing among Federal agencies.

   B. DHS information sharing with regions, States, and municipalities has improved through mechanisms such as fusion centers.

   C. There is a sound foundation for effective information sharing with the private sector through the Critical Infrastructure Partnership Advisory Council, the Sector Coordinating Councils, the National Infrastructure Protection Plan, the National Response Framework, and the Information Sharing Environment.

Foundation 2

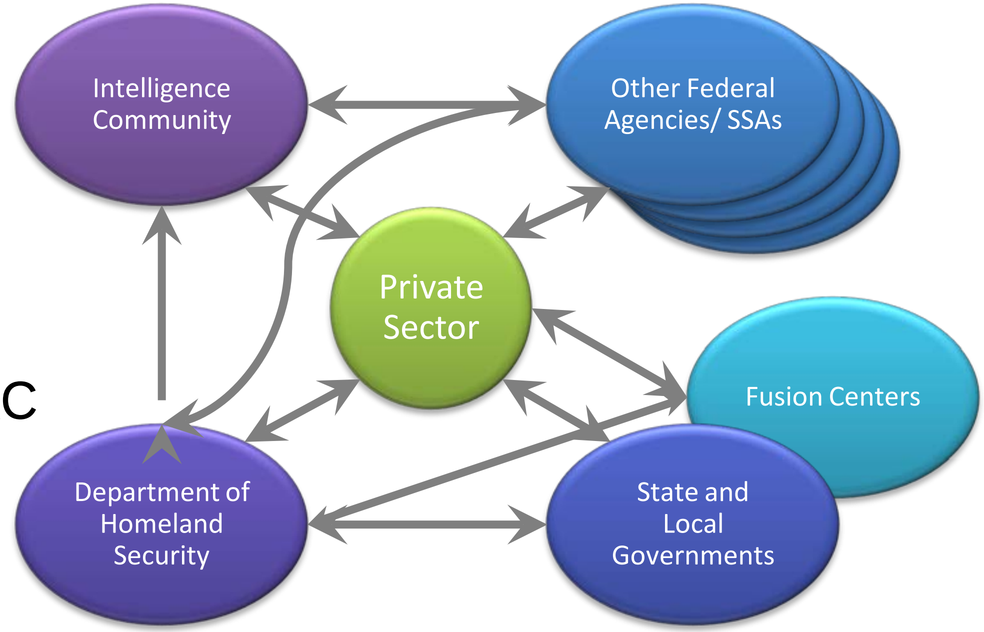
2. **The Council reaffirms that voluntary public-private partnership is the best long-term strategy to secure our critical infrastructures.**

   A. Regulations and standards, if developed wisely with the full collaboration of the regulated private sector entities, have their place in protecting critical infrastructures.

   B. A non-regulatory approach, which encourages industry and government to diligently pursue common national infrastructure protection goals while avoiding unnecessary costs and inefficiencies, is preferred and in the best interests of the Nation.

A Complicated Problem

- Information sharing is complex
  - Multiple organizations
  - Multiple tiers of people
  - Multiple sharing pathways
  - Physical and cyber elements
  - Multiple “rules of the road”
- Studied extensively by NIAC and others
- Solutions must address underlying root causes as well as the symptoms that result in information sharing breakdowns


Intelligence Community
Other Federal Agencies/ SSAs
Private Sector
Fusion Centers
Department of Homeland Security
State and Local Governments

Findings and Recommendations

- Key Messages
- Summary of Recommendations
- Detailed Findings and Recommendations
  1. Authority and Policy
  2. Implementation of Authority
  3. Leveraging Partner Capabilities to Reduce Risk
  4. Information Content
  5. Information Delivery
  6. Counterintelligence/counterterrorism
  7. Fusion Centers

Key Messages

1. The public-private component of the **infrastructure protection mission is not receiving the high priority** that is commensurate with its vital importance to the Nation’s economic health and security.
2. The unique knowledge and analysis **capabilities offered by the private sector are not widely understood** by government and the processes to leverage these capabilities are not in place.
3. Public and private sector **incentives for sharing information are not aligned** to serve a common infrastructure protection mission.
4. The Federal **intelligence sharing enterprise is complex** and often confusing.
5. The Department of Homeland Security **(DHS) is not serving as an effective champion** and leader for the intelligence sharing interests of the private sector for the overall infrastructure protection mission within the Federal government.

Summary of Recommendations

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

Finding 1
Authority and Policy

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

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

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

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

Recommendation 1

Assert the Priority of Infrastructure Protection and Resilience in National Security

A. The White House should vigorously affirm the criticality of infrastructure protection and resilience to our Nations' security and our citizen's well being through policy emphasis that drives action. Through a Presidential Policy Directive or other policy mechanism, the White House should direct DHS and the Intelligence Community to: weigh issues of harm to critical sectors against other missions in all operations, collect infrastructure intelligence needs and evaluate terrorist targets in the critical sectors, and prepare a quadrennial report on infrastructure protection intelligence sharing.

B. The White House should employ current or new partnership mechanisms for senior executives in the private sector to engage their government counterparts to facilitate a truly National approach that *leverages public-private resources* for large-scale, persistent threats.

Finding 2
Implementation of Authority

A. DHS's implementation of its authority is uneven, reflecting an early stage of maturity in an evolving model for information sharing.

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

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

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

Recommendation 2

Improve the Implementation and Accountability of Existing Authorities

To improve performance and accountability and help mature DHS's role as a member of the Federal Intelligence Community, the NIAC recommends:

A. The Office of the Director of National Intelligence (ODNI) assist DHS in developing, modifying, or assessing programs and processes for private sector information sharing.

B. DHS reexamine the effectiveness of its risk management organizational structure, specifically the separation of threat analysis (in the Office of Intelligence and Analysis) from vulnerability and consequence analysis (in the Office of Infrastructure Protection).

C. DHS, supported by ODNI, establish core teams of 3-4 intelligence specialists specifically for each sector, and one team focused on cross-sector information issues.

D. ODNI aim to reduce ambiguity and simplify engagement points and processes in the rules and relationships for information sharing.

E. The President define the functions (and authority to execute them), expected outcomes, and accountability measures for Sector-Specific Agencies (SSAs).

Finding 3
Leveraging Partner Capabilities

A. The special capabilities of the private sector are not widely understood by government and the processes to leverage this capability are not in place.

B. Different incentives within the Federal Intelligence Community and the private sector make it difficult to define a shared value proposition that encourages information sharing.

C. Intelligence-sharing mechanisms between the private sector and the Federal government are complicated, at times confusing, and may be redundant and/or conflicting.

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

E. Successful models of bi-directional intelligence information sharing exist, including a recently initiated DHS pilot effort with the Banking and Finance Sector to define intelligence-sharing protocols.

F. Some Sector Coordinating Councils (SCCs) have been successful in defining their informational needs and working with their Sector Specific Agency to companion their sector's intelligence needs.

Recommendation 3
Improve Information Content by Leveraging Partner Capabilities to Reduce Risk

A. DHS should work with each Sector-Specific Agency to implement, for all 18 critical infrastructure sectors, a robust intelligence requirements process that 1) meets the information needs of owners and operators, 2) delivers these requirements to appropriate elements of the Federal Intelligence Community, 3) is consistent with existing Intelligence Community processes, and 4) supports advocacy for critical infrastructure priority within the Intelligence Community.

B. To support these requirements, DHS should develop a more robust and timely analysis capability that leverages knowledgeable personnel and enhanced analytical resources for each critical infrastructure sector, to support sector-specific needs, business models, and risk-management processes. DHS should leverage commercially-available tools and techniques to provide capabilities for predictive intelligence for critical infrastructure protection.

Finding 4
Information Content

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

B. Fragmentary intelligence information can be valuable to the private sector. Such information, while not always important for the Federal Intelligence Community, may be very relevant for private sector security operations.

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

D. DHS is in the nascent stages of using predictive analytics. In comparison, the Federal Intelligence Community and the private sector make effective use of these tools.

Recommendation 4
Improve the Value of Information Products to Industry Risk-Management Practices

A. The Office of the Director of National Intelligence (ODNI), working jointly with DHS, should establish new intelligence dissemination product formats to create tailored and practical products that help owners and operators protect assets and improve business continuity. DHS and its Federal intelligence partners should supplement classified threat briefings with unclassified reports that can be readily and broadly shared.

Finding 5
Information Delivery

A. Intelligence sharing processes, tools, and products are improving, but need to be significantly better.

B. The current usefulness of the Homeland Security Information Network – Critical Sectors (HSIN-CS) as a preferred mechanism for sharing is modest at best. However, the recent DHS business-case assessment for HSIN is driving to remediate deficiencies.

C. The private sector uses multiple sources to meet its intelligence needs, including trusted personal relationships, trade associations, various DHS components, other government agencies, Sector Specific Agencies, Information Sharing and Analysis Centers, fusion centers, and State and local law enforcement.

D. The Critical Infrastructure Protection Advisory Council (CIPAC) structure is an essential foundation for effective information sharing. As part of this foundation, trade associations play an essential role in information sharing and in some cases the only formal mechanism for small and medium-sized businesses.

Recommendation 5
Build Accepted Practices for Timely Information Delivery

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

B. DHS should guide Homeland Security Information Network – Critical Sectors (HSIN-CS) implementation to ensure: 1) sectors are better educated that their needs drive system requirements, 2) system implementation is based on and measured by understanding and meeting these user needs, and 3) system architecture takes advantage of state-of-the-art, commercially available tools for threat analysis in order to meet these needs in a timely manner.

Finding 6
Counterintelligence/ Counterterrorism

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

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

Recommendation 6
Capitalize on Private Sector Capabilities for Counterterrorism Solutions

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

Finding 7
Fusion Centers

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

Recommendation 7
Enhance Fusion Center Capabilities as One Mechanism for Sharing

A. Where appropriate, DHS should guide fusion centers to establish an information sharing function with owners and operators as part of a critical infrastructure protection and resilience mission. DHS should support—through funding, personnel, training, technology, and analytic tools—the development of an infrastructure protection and resilience capability that could stand alone or be integrated within fusion centers to facilitate the flow of intelligence information to and from the private sector, while ensuring information protection and addressing privacy concerns.

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

Discussion and Questions

Questions?