

# National Infrastructure Advisory Council (NIAC)



## Intelligence Information Sharing Study: Working Group Status Update to the Full Council

**July 12, 2011**

Al Berkeley  
Chairman,  
Pipeline Trading Systems LLC

Philip G. Heasley  
President and Chief  
Executive Officer,  
ACI Worldwide

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

# Overview

---

- Study Leadership
- Background
- Tasking to the NIAC: Three Aspects
- The Challenge this Study Addresses
- Study Approach
- Authorities and Information Sharing Strategies
- Building on Current Tools
- Progress to Date
- General Observations
- Initial Findings
- Next Steps
- Questions?

# Study Leadership

---

- Working Group Co-Chairs:
  - **Al Berkeley**, Chairman, Pipeline Trading Systems
  - **Phil Heasley**, President & CEO, ACI Worldwide
  - **Jim Nicholson**, President & CEO, PVS Chemicals
- Working Group Members:
  - **Wes Bush**, President & COO, Northrop Grumman
  - **Jim Reid**, President, CB Richard Ellis Eastern Division
  - **Mike Wallace**, Former Vice Chairman & COO, Constellation Energy

# Study Leadership (Study Group Members)

---

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

# Background

---

- At the April 13, 2010 NIAC Quarterly Business Meeting, the Department of Homeland Security (DHS) requested that the Council conduct an updated study on intelligence information sharing.
- DHS requested that this proposed study include an examination of the previous findings and recommendations from the 2006 NIAC *Report on Public-Private Sector Intelligence Coordination* as well as the review of new policies and programs, including fusion centers.
- The NIAC approved the study approach at the October 19, 2010 Quarterly Business Meeting.

# Tasking to the NIAC: Three Aspects

---

1. Intelligence information sharing, addressing:
  - The timeliness and relevance of information and intelligence shared between the public and private sectors.
  - The effectiveness of bi-directional processes and products for sharing between government and the private sector.
2. Enhancing owner and operator contributions to counterintelligence, addressing:
  - The private sector role in counterintelligence.
  - Challenges and potential solutions to improving contributions by owners and operators.
3. The role of fusion centers, addressing:
  - Private sector participation and interaction.
  - Information sharing challenges, gaps, and best practices.

# The Challenge this Study Addresses

---

- Mission-driven, bi-directional intelligence information sharing between the Federal government and infrastructure owners/operators is a new paradigm that requires an adaptive and flexible model much different than the Federal-centric, cold-war model still common in the intelligence community.



# The Challenge this Study Addresses

---

- This new model has been slow to develop and mature because it inherently:
  - Challenges the Intelligence and Law Enforcement Communities to disseminate sensitive information to a new customer and to prioritize collection and analysis in new ways.
  - Requires the Federal government and the private sector to spend significant time and resources building trusted partnerships and information sharing processes.
- Addressing this challenge is imperative:
  - Critical infrastructure is central to the Nation's economic security, which itself is a vital element of the Nation's national security.
  - As critical infrastructure systems become more complex and interdependent, sector vulnerabilities to-and consequences from- disruptions will continue to increase.

# Study Approach: Build on Prior NIAC Work

---

- 2006 NIAC *Report on Public-Private Sector Intelligence Coordination*:
  - Strongly supports need for sector-specific frameworks for information sharing.
  - Recommends the development of bi-directional, sector-specific processes for sharing intelligence information with private sector.
- 2008 *Critical Infrastructure Partnership Assessment*:
  - Recommends the ability for sectors to articulate a variety of sector needs, identify sector priorities, and implement strategies.

# Study Approach: Information Content and Sources

---

- Study examines the different stages of information sharing including requirements generation, information gathering, analysis and dissemination.
- The perspectives of chief executives and subject matter experts in business and government are providing the primary sources of information.
  - These engagements will provide the basis for the study findings and proposed recommendations.
- Additional information is being obtained from a comprehensive examination of open source material.

# Study Approach: Sector Case Studies

---

- Five sectors have been selected for in-depth case studies:
  - Commercial Facilities, Healthcare and Public Health, Oil and Natural Gas Segment of the Energy Sector, Banking and Financial Services, and Chemical.
- The case-study examinations:
  - Identify sector-specific characteristics and approaches to intelligence sharing.
  - Illustrate examples of bi-directional information sharing successes and areas in need of improvement.
  - Provide sector-specific observations and findings.
- Case-study information is being synthesized and assessed to:
  - Identify common characteristics, trends, and gaps in intelligence information sharing.
  - Inform study-wide findings and potential recommendations.

# Critical Infrastructure: Authorities and Information-Sharing Strategies

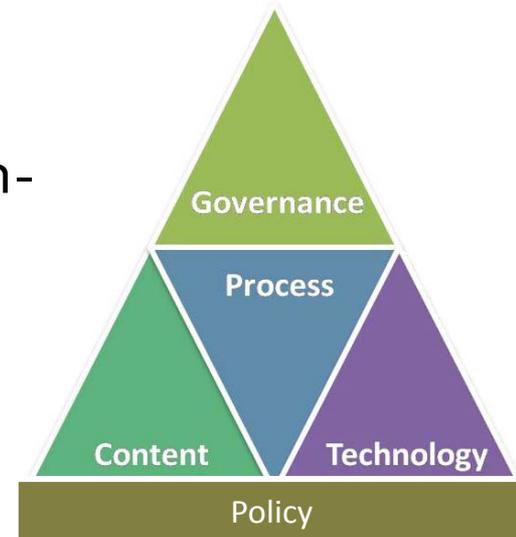
---

- Various legislative authorities guiding intelligence information sharing include the Homeland Security Act and the Intelligence Reform and Terrorism Prevention Act
- National Infrastructure Protection Plan:
  - Unifying National program guiding critical infrastructure protection and resilience efforts.
- National Information Sharing Strategy – articulates the guiding principles for the National Information Sharing Environment (ISE):
  - National ISE Program Manager, Office of the Director of National Intelligence (ODNI), designated the DHS Office of Infrastructure Protection as the Executive Agent for integrating the CIKR private sector as users into the ISE through the CIKR ISE.
  - The Critical Infrastructure and Key Resources (CIKR) ISE and other elements of the National ISE, such as Fusion Centers, likely are key parts of any solution.

# Building on Current Tools

---

- There are current structures and processes that can be building blocks for maturing critical information sharing processes
- For example, the CIKR ISE is a useful construct to guide the maturity of information-sharing processes against five elements:
  - Policy – legal authorities
  - Governance – roles, responsibilities
  - Process – capabilities that define info sharing
  - Technology – platforms that enable sector communication and coordination.
  - Content – formalized process that defines information that is required, generated, and received by sector members and other stakeholders.



# Progress to Date

---

- Over 125 interviews, briefings, and executive roundtables have been conducted, involving:
  - Chief executives and private sector owners/operators.
  - Subject matter experts.
  - Federal agency representatives, including the intelligence community.
  - Critical Infrastructure Partnership Advisory Council sector council members.
- Multiple patterns of intelligence sharing have been identified across the five case-studies.
  - Reflects the diversity of business models, risk-management practices, and varying degrees of maturity in the evolving model of bi-directional sharing.
  - Role of all hazards information sharing.
- Study-wide general observations and initial findings have been developed.

# General Observations: Federal Partner

Mission	<ul style="list-style-type: none"><li>▪ <b>Intelligence information flow from the Federal government to the private sector is vital to the security and resilience of critical infrastructure.</b><ul style="list-style-type: none"><li>▪ Most government agencies accept the new paradigm of sharing intelligence information with the private sector, but a culture change is difficult.</li></ul></li><li>▪ <b>The mission of a Federal organization has a critical effect on intelligence information sharing.</b><ul style="list-style-type: none"><li>▪ The Federal Intelligence Community serves multiple customers with widely disparate missions, including diplomacy, law enforcement, military force protection, homeland security and critical infrastructure protection – and information priorities must be balanced among these missions.</li></ul></li></ul>
Maturity	<ul style="list-style-type: none"><li>▪ <b>Bi-directional flow between the Federal government and the private sector is an <i>evolving</i> model, with widely varying degrees of engagement and implementation by DHS and the various Sector Specific Agencies (SSAs).</b></li><li>▪ <b>Continued improvements in information sharing structures and processes are essential and must be implemented through personnel having appropriate judgment and expertise.</b></li><li>▪ <b>Overall, effective intelligence information flow remains at an early stage of maturity.</b></li></ul>
Effectiveness	<ul style="list-style-type: none"><li>▪ <b>While intelligence information sharing has improved since 2006, there are many areas in which major improvements are still needed.</b><ul style="list-style-type: none"><li>▪ Many CIKR sectors believe that the government does not understand what their critical infrastructure protection information requirements are, and current government intelligence products are of limited value.</li><li>▪ Multiple redundant government sources of intelligence information create confusion and dilute the impact.</li><li>▪ Effective bi-directional sharing requires a government feedback mechanism.</li><li>▪ Linking the right people with the right information at the right time is a paradigm that involves new requirements and complex relationships and will take time to develop.</li></ul></li></ul>

# General Observations: Private Sector Partner

Mission	<ul style="list-style-type: none"><li>▪ <b>Information flow from the private sector to the Federal government is also vital to the security and resilience of critical infrastructure.</b><ul style="list-style-type: none"><li>▪ By and large, the private sector understands this and is willing to share its information with the government.</li></ul></li></ul>
Maturity	<ul style="list-style-type: none"><li>▪ <b>This is an <i>evolving</i> model, with widely varying degrees of understanding and engagement among the various sectors.</b></li><li>▪ <b>Trusted, personal relationships are used extensively by the private sector.</b><ul style="list-style-type: none"><li>▪ Relationships are time tested and will remain an important part of intelligence information sharing.</li><li>▪ These should not replace improved structures and processes designed for the private sector community as a whole.</li></ul></li><li>▪ <b>The experiences of sectors in sharing with the Federal government are often quite different.</b><ul style="list-style-type: none"><li>▪ This reflects the nature of differing sector assets (physical and cyber, open and closed facilities), business models, risk-management, and history of collaboration.</li></ul></li></ul>
Effectiveness	<ul style="list-style-type: none"><li>▪ <b>Intelligence information sharing has improved since 2006, but improvements are still needed.</b><ul style="list-style-type: none"><li>▪ The flow of information from the private sector to the government is substantial and growing.</li><li>▪ It is not clear that the government values information provided by the private sector or is able to act on it in a timely manner.</li><li>▪ Linking the right people with the right information at the right time requires some refocusing of existing law, structures, staff, training and/or incentives for many sectors to realize systemic improvement – and will take time to develop.</li></ul></li></ul>

# Initial Findings: Federal Partner

---

- Federal law and policy clearly includes the private sector as a customer of the Federal intelligence community.
- DHS has the clear authority to coordinate the sharing of homeland security information between the Federal government and the private sector.
- Implementation of this authority reflects an early stage of maturity of an evolving model for information sharing.
  - Translating this paradigm into effective practice is a significant challenge to the Federal government, where the practices necessary to ensure *operational* success appear to either not be in place or not well developed.
  - Diverse sector operations require multiple credible flows/channels of information delivery.

# Initial Findings: Federal Partner (con't)

---

- Federal processes and resources are not yet at a sufficient level of maturity to:
  - Adequately reflect the private sector critical infrastructure protection information needs in the Intelligence Community's collection requirements generation process. This leads to major shortcomings in the relevance of intelligence products disseminated to the private sector.
  - Effectively engage 18 critical infrastructure sectors in determining critical infrastructure needs for intelligence information.
  - Implement operational processes for rapid, targeted dissemination of intelligence information.
  - Serve as an effective advocate for critical infrastructure intelligence needs within the Federal intelligence community.
- Sector Specific Agencies (SSAs) vary significantly in the extent and effectiveness of the role as a bridge between an individual sector and the Federal intelligence community.

# Initial Findings: Private-Sector Partner

---

- The private sector generally does not receive the intelligence information they need, though this varies somewhat across sectors.
  - With the exception of asset-specific threats, the majority of information received is reactive to events rather than usefully proactive.
- Predictive analysis (i.e. predictive analytics) is needed so that responsible parties may be proactive in protecting critical infrastructure.
- The majority of information received through formal mechanisms does not meet owner/operator needs.
  - Instances of aligning the right people, time, and information are in the minority of engagements.
- The private sector more readily embraces the bi-directional model.
  - Unlike the Federal intelligence community, the private sector does not have multiple mission areas or the legacy of the traditional model.

# Initial Findings:

## Private-Sector Partner (continued)

---

- Engagement points and intelligence information-sharing mechanisms with the Federal government are complex, confusing, and may be redundant and conflicting.
  - As a result, engagement through trusted relationships remains a primary means of facilitating the flow of needed intelligence information.
- Similar to SSAs, the extent and effectiveness of private sector engagement with Federal government partners varies significantly.
  - There are emerging models of success in bi-directional sharing.
  - These models may differ substantially depending upon the nature of sector assets, interdependency, business models, risk-management processes, and relationships.

# Initial Findings: Counterterrorism

---

- Counterterrorism vs. counterintelligence as the practical focus of the private sector.
  - This study found that the term "counterintelligence" has specialized meaning in the intelligence community that is mainly outside of the role of the private sector.
  - This study also found that the term "counterterrorism" is a more accurate term for what the private sector is attuned to and to which it can contribute.
  - Accordingly, the study will use the term "counterterrorism" going forward.
- The private sector believes it has a unique, value-added role in providing this type of information.

# Initial Findings:

## Counterterrorism (Continued)

---

- In most cases, the private sector is willing and able to provide such information.
  - This requires trust that the information is valued and acted upon.
- Government feedback is critical to encourage and direct this information flow.
  - Was the information viewed as useful?
  - Was it in fact used?
  - What was the outcome?
  - How can private-sector input be improved?

# Initial Findings: Fusion Centers

---

- The fusion-center mechanism appears to be effective for the law enforcement and first-responder engagement with State, regional, and local communities consistent with its primary mission.
- The use of fusion centers for sharing with the private sector varies widely across locations and sectors, but overall seems comparatively modest.
  - There are, however, several good models of success in this regard.
- *As a mechanism for leveraging resources* across partners, the fusion center appears to be a highly effective model.
- The absence of critical infrastructure protection as a key mission, as well as State laws that govern information protection, appear to be current constraints.
- Fusion centers are likely one of several mechanisms that may address critical infrastructure needs, recognizing that both *needs and resources* vary according to location.

# Next Steps

---

- Complete follow-up interviews and other investigative engagements to clarify, as needed, the understanding of specific intelligence information-sharing processes and their effectiveness.
- Develop study-wide set of potential actionable recommendations, focused on four key structural areas:
  1. Are the appropriate laws, policies, regulations, and authorities in place to clearly define Federal intelligence-information sharing responsibilities with the private sector critical infrastructure owners and operators, and is there any confusion, redundancy, or conflict among these for the multiple federal agencies with intelligence information-sharing responsibility?

# Next Steps (continued)

---

- Develop study-wide set of potential actionable recommendations, focused on four key structural areas (continued):
  2. What actions must be implemented to ensure Federal intelligence products are aligned with and timely for private sector risk-management processes, including sector-defined requirements?
  3. What actions must be taken to ensure the Federal intelligence community and the private sector understand and complement each other's intelligence capabilities to mutual benefit?
  4. What improvements can be made in the bi-directional processes that enable the timely sharing of data and analyzed information between the Federal intelligence community and the private sector?

# Questions

---

Questions?