Lesson 5 Outline

Course Number: XXXX

Course: Foundations of Critical Infrastructure Security and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

LESSON 5 TOPIC: ORGANIZING AND PARTNERING TO SHARE INFORMATION

1. Lesson Goals/Objectives:

- Understand and be able to discuss the core elements of National-level CISR-related information sharing policy.
- Identify and assess the different structures, methods, processes, and systems that the various NIPP partners use to share information with one another.
- Discuss how CISR-related information is collected, warehoused, protected, and exchanged among various levels of government and the private sector.
- Evaluate the ongoing challenges and barriers to information sharing and collaboration that exist among the various levels of government, as well as between government and the private sector.

2. Discussion Topics:

- What are the principal types and sources of information that support the CISR mission?
- What are the core elements of CISR-related information sharing policy as discussed in national policy and strategy?
- How do the various elements of the NIPP Partnership Model interact with one another to share all-hazards information?
- How effective is the NIPP Partnership Model in achieving the necessary level and quality of information sharing required to execute the CISR mission?
- What are the roles and responsibilities of the U.S. Department of Homeland Security (DHS); the Federal Bureau of Investigation (FBI); and the State, local and regional fusion centers regarding CISR-related information sharing and analysis?
- What are the Information Sharing and Analysis Centers (ISACs)? How do they interact with government?
- What are the key processes and systems used to share CISR -related data, to include intelligence-related information, among the various stakeholders nationally, regionally, and locally?
- How is classified national security information shared between government and industry? How and from whom does industry receive terrorism-related information?
- How do government and industry work together to protect sensitive information? Are there areas for improvement?
- What does E.O. 13691, *Improving Private Sector Information Sharing*, have to say

regarding the sharing of cybersecurity threat information within the private sector and between the private sector and government? What are the core elements of the framework laid out therein to help private sector entities work together, as well as with the Federal Government, to quickly identify and protect against cyber threats?

- How is CISR-related information and intelligence that originate from multiple distributed sources compiled and deconflicted? Are we successfully "connecting the dots" today?
- What are the principal barriers to sharing information proactively and comprehensively between government and industry at all levels of the NIPP partnership?
- How have real-world successes/failures led to improvements in information sharing among government and industry partners?

3. In-class Exercise: Learners will be organized into 3-4 person teams and will be prepared to discuss CISR-related information sharing in the context of a specific incident type (i.e. major hurricane, terrorist attack, major winter storm, power blackout, HAZMAT release, etc.). The discussion will focus on incident-specific CISR roles, responsibilities, and relationships; type and sources of information typically shared; mechanisms and systems used to share information; impediments to information sharing in the context of the incident type assigned, etc.

4. Required Reading:

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, Appendix A, http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf.

National Strategy for Information Sharing and Safeguarding, 2012, http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.

The White House, Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing*, March 2015, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

A Policy Framework for the ISAC Community, 2004, http://www.isaccouncil.org/images/Policy_Framework_for_ISAC_Community_013104.pdf.

A Functional Model for Critical Infrastructure Information Sharing and Analysis, 2004, http://www.isaccouncil.org/index.php?option=com_docman&task=doc_view&gid=9&Itemid=208.

The Role of ISACs in Private/Public Sector CIP, 2009, http://www.isaccouncil.org/images/ISAC_Role_in_CIP.pdf.

National Infrastructure Advisory Council, *Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations*, 2008, http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf.

U.S. Government Accountability Office, *Homeland Security: Federal Efforts are Helping to Address Some Challenges Faced by State and Local Fusion Centers*, 2008, http://www.gao.gov/new.items/d08636t.pdf.

Robert Riegle, Testimony, *The Future of Fusion Centers: Potential Promise and Dangers*, 2009, http://www.dhs.gov/ynews/testimony/testimony_1238597287040.shtm.
Information Sharing and the Private Sector, http://www.ise.gov/sharing-private-sector.

Information Sharing Environment, http://itlaw.wikia.com/wiki/Information_Sharing_Environment.

4. Recommend Additional Reading:

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 2013, 11(10), pp. 1-8, 16-21, 2013, http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/April2013_PartershipsInformationSharing.pdf.

CIKR Resource Center, *CIKR Partnerships*. http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/CIKRpartnerships.htm.

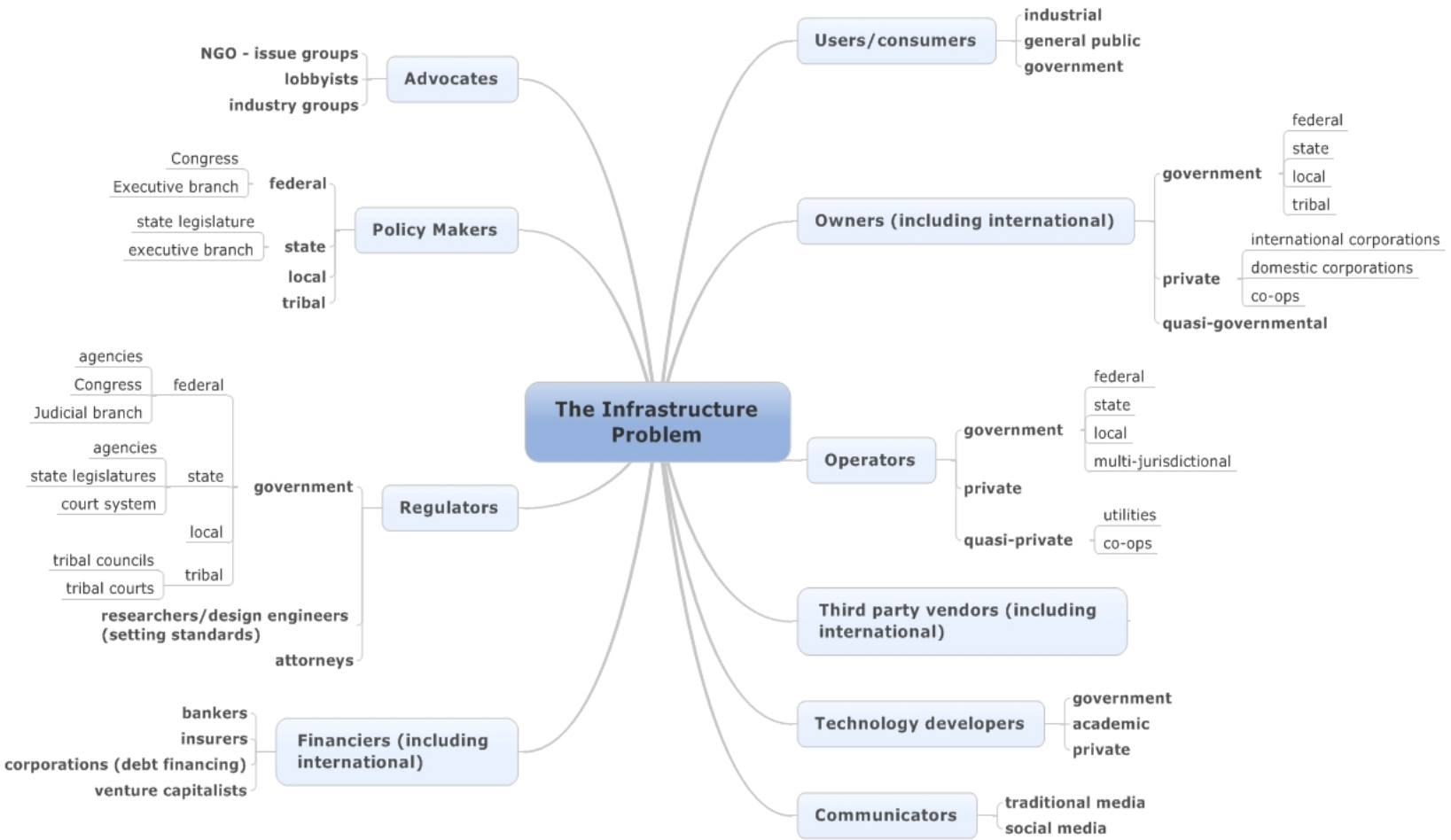
Foundations of Critical Infrastructure Security and Resilience

Lesson 5: Organizing and Partnering to Share Information

Lesson 5 Objectives

- Understand and be able to discuss the core elements of National-level CISR-related information sharing policy.
- Identify and assess the different structures, methods, processes, and systems that the various NIPP partners use to share information with one another.
- Discuss how CISR-related information is collected, warehoused, protected, and exchanged among various levels of government and the private sector.
- Evaluate the ongoing challenges and barriers to information sharing and collaboration that exist among the various levels of government, as well as between government and the private sector.

The CISR Community: “Who Plays in the Space”



Information Sharing: An Evolving Challenge

- The “4 Ps”: Connecting People, Processes, Products and “Pipes”
- Information sharing is complex
  - Multiple organizations
  - Multiple tiers of people
  - Multiple types of info to be shared; end-user requirements vary
  - 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

Sharing Intelligence Info with the Private Sector

- The private sector is an evolving 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

NIAC Report – January 2012 – Key Message

- 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.
- 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.
- Public and private sector **incentives for sharing information are not aligned** to serve a common infrastructure protection mission.
- The Federal **intelligence sharing enterprise is complex** and often confusing.
- 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.

NIAC Report – Finding 1

- Federal law and policy clearly include the private sector as a customer of the Federal Intelligence Community.
- DHS has clear authority to share with the private sector the counterterrorism and CISR info developed by the Federal Intelligence Community.
- 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.
- 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.

NIAC Report – Recommendation 1

- The White House should vigorously affirm the criticality of CISR to our Nations' security and our citizens' 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 Intel Community to: weigh issues of harm to critical sectors against other missions in all operations, collect infrastructure intel needs and evaluate terrorist targets in the critical sectors, and prepare a quadrennial report on infrastructure protection intelligence sharing.

- 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.

- Source: National Infrastructure Advisory Council, *Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations*, 2008

NIAC Report – Finding 2

- DHS's implementation of its authority is uneven, reflecting an early stage of maturity in an evolving model for info sharing.
- The Federal Intel Community often does not understand what info the private sector needs, nor does the private sector always understand the actual capabilities and missions of the Intel Community.
- 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 intel information in overall public-private risk-management processes.
- The complexity of roles and responsibilities in the Federal intel-sharing enterprise is confusing to the private sector, and it lacks the clarity needed to be truly effective.

NIAC Report – Recommendation 2

- The Office of the Director of National Intelligence (ODNI) assist DHS in developing, modifying, or assessing programs and processes for private sector information sharing.
- 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).
- 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.
- ODNI aim to reduce ambiguity and simplify engagement points and processes in the rules and relationships for information sharing.
- The President define the functions (and authority to execute them), expected outcomes, and accountability measures for Sector-Specific Agencies (SSAs).

NIAC Report – Finding 3

- The special capabilities of the private sector are not widely understood by government and the processes to leverage this capability are not in place.
- Different incentives within the Federal Intel Community and the private sector make it difficult to define a shared value proposition that encourages info sharing.
- Intel-sharing mechanisms between the private sector and the Federal government are complicated, at times confusing, and may be redundant and/or conflicting.
- The private sector is willing and able to share info with government that may be useful in counterterrorism ops. However, the government may not yet be prepared to receive info from the private sector, to act on it, or to provide feedback on its usefulness.

NIAC Report – Recommendation 3

- DHS should work with each SSA to implement a robust intel requirements process that 1) meets the info needs of owners and operators, 2) delivers these requirements to appropriate elements of the Federal Intel Community, 3) is consistent with existing Intel Community processes, and 4) supports advocacy for critical infrastructure priority within the Intel Community.

- DHS should develop a more robust and timely analysis capability that leverages knowledgeable personnel and enhanced analytical resources for each CI 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 intel for critical infrastructure protection.

NIAC Report – Finding 4

- The private sector generally does not receive the intel info it needs, though this varies somewhat across sectors. The majority of info received is reactive to events rather than usefully predictive.
- Fragmentary intel info can be valuable to the private sector. Such information, while not always important for the Federal Intel Community, may be very relevant for private sector security ops.
- 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.
- DHS is in the nascent stages of using predictive analytics. In comparison, the Federal Intel Community and the private sector make effective use of these tools.

NIAC Report – Recommendation 4

- The Office of the Director of National Intelligence (ODNI), working jointly with DHS, should establish new intel 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 unclass reports that can be readily and broadly shared.

NIAC Report – Finding 5

- Intel sharing processes, tools, and products are improving, but need to be significantly better.
- 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.
- The private sector uses multiple sources to meet its intel needs, including trusted personal relationships, trade associations, various DHS components, other government agencies, SSAs, ISACs, fusion centers, and State/local law enforcement.
- The CIPAC structure is an essential foundation for effective information sharing. As part of this foundation, trade associations play an essential role in info sharing and in some cases the only formal mechanism for small and medium-sized businesses.

NIAC Report – Recommendation 5

- 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 CI intel info sharing pathways and 2) establish sector-specific intel info sharing protocols with the specific goal of improving timeliness. DHS and the SSAs should work with the SCCs 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 intel info sharing.

- DHS should guide 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.

NIAC Report – Finding 6

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

- 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.

NIAC Report – Recommendation 6

- The Federal Government should capitalize on the info 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 info on which the sectors should focus, and update these areas on a regular basis as conditions dictate.

EO 13636 – Improving Critical Infrastructure Cybersecurity

- Policy: Increase volume, timeliness, and quality of cyber threat info shared w/ U.S. private sector entities so that they may better protect themselves against cyber threats.
  - AG, DHS Sec and DNI to ensure timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity…and develop process to rapidly disseminate reports to targeted entity. Process also to include dissemination of classified reports to CI entities authorized to receive them.
  - DHS Sec in collaboration with SECDEF to establish procedures expanding Enhanced Cybersecurity Services program to all CI sectors to provide classified cyber threat/technical info from Govn't to eligible CI companies or commercial service providers offering security services to CI entities.
  - DHS Sec to expedite processing of security clearances for appropriate personnel employed by CI owners/operators, and expand use of programs bringing private sector SMEs into Federal service on a temporary basis.

EO 13691 – Improving Critical Infrastructure Cybersecurity

- Policy: Order encourages voluntary formation of organizations sharing info related to cyber risks/incidents, establishment of mechanisms to continually improve their capabilities and functions, and their partnering with the Fed Govn't on a voluntary basis.
  - DHS Sec to strongly encourage development and formation of Information Sharing and Analysis Organizations (ISAOs).
  - ISAOs to be organized on the basis of sector, sub-sector, region, or other affinity, including in response to particular emerging threats or vulnerabilities. Membership drawn from public or private sectors, or a combination of public and private sector organizations. May be formed as for-profit or nonprofit entities.
  - NCCIC to engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of cyber risk information.
  - DHS Sec to consult with other Federal entities responsible for conducting cybersecurity activities, including Sector-Specific Agencies, independent regulatory agencies at their discretion, and national security and law enforcement agencies.
  - DHS Sec to work through a nongovernmental organization to serve as the ISAO Standards Organization (SO), which shall identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs under this order.

NIPP 2013 Call to Action

- **Call to Action #5: Enable Risk-Informed Decision Making through Enhanced Situational Awareness**

- Improve practices for sharing info and applying knowledge gained through changes in policy, process, and culture and promote a culture of "need to share" and "responsibility to provide," recognizing that CI owners/operators and SLTT govnts are crucial consumers *and* providers of risk information.

- Consult with SLTT governments and owners/operators to ensure that intel analyses meet their needs, and exercise consistent means for disseminating intel/info products.

- Enhance NICC, NCCIC, and other Federal info-sharing resources' ability to produce and share cross-sector, near real-time situational awareness while protecting sensitive info.

- Leverage "tearline" and "shareline" policies and procedures to facilitate sharing of actionable portions of otherwise classified or restricted unclassified reports with private sector and SLTT partners.

National Strategy for Info Sharing and Safeguarding

- Provides guidance for effective development, integration, and implementation of policies, processes, standards, and technologies to promote secure and responsible info sharing.

- 3 Core principles:
  - Information as a National Asset
  - Info Sharing and Safeguarding Requires Shared Risk Management
  - Info Informs Decision making

- 5 goals:
  - Drive Collective Action through Collaboration and Accountability
  - Improve Information Discovery and Access through Common Standards
  - Optimize Mission Effectiveness through Shared Services and Interoperability
  - Strengthen Information Safeguarding through Structural Reform, Policy, and Technical Solutions
  - Protect Privacy, Civil Rights, and Civil Liberties through Consistency and Compliance

Discussion Questions: Information Sharing

- What are the key elements of the *National Strategy for Information Sharing and Safeguarding*? How does the CSIR mission area fit into this strategy?
- What are the motivations/incentives that drive government-private info sharing? What are the criteria used by the private sector to assess the value of collaborative info sharing with the public sector at various levels?
- What are the principal types and sources of information that support the CSIR mission?
- What are the key processes and systems used to share CSIR-related data, to include intel info, among the various CI stakeholders nationally, regionally, and locally?
- How effective is the NIPP Partnership Model in achieving the necessary level and quality of info sharing required?
- What are the Information Sharing and Analysis Centers (ISACs)? How do they interact with government?
- What are the principal barriers to sharing info proactively and comprehensively between govn't at all levels of the NIPP partnership?

Discussion Questions (Cont.)

- How is classified national security info shared between government and industry? How and from whom does industry receive terrorism-related info?
- How do govn't and industry work together to protect sensitive info? How could this process be improved? How has the Eric Snowden incident impacted this relationship?
- How is CI-related info originating from multiple distributed sources compiled and deconflicted? Are we successfully "connecting the dots" today?
- What does E.O. 13691, *Improving Private Sector Information Sharing,* have to say regarding the sharing of cybersecurity threat information within the private sector and between the private sector and government? What are the core elements of the framework laid out therein to help private sector entities work together, as well as with the Federal Government, to quickly identify and protect against cyber threats?

In-class Activity

- Learners will be organized into 3-4 person teams and will be prepared to discuss CISR-related information sharing in the context of a specific incident type (i.e. major hurricane, terrorist attack, major winter storm, power blackout, HAZMAT release, etc.). The discussion will focus on incident-specific CISR roles, responsibilities, and relationships; type and sources of information typically shared; mechanisms and systems used to share information; impediments to information sharing in the context of the incident type assigned, etc.