Lesson 4 Outline

Course Number: XXXX

Course: Foundations of Critical Infrastructure Security and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

LESSON 4 TOPIC: EXAMINING CISR AUTHORITIES, ROLES, AND RESPONSIBILITIES: FEDERAL, SLTT, AND PRIVATE SECTOR

****Special Activity: Incident management exercise roles assigned by Instructor/Professor**

1. Lesson Goals/Objectives:

- Identify and describe the various public and private sector components of the NIPP Partnership Framework.
- Identify the various key stakeholders within the CISR mission space and discuss the authorities, roles, and responsibilities of each.
- Evaluate the principal political, organizational, legal, and resource challenges that those responsible for CISR face in executing those responsibilities.

2. Discussion Topics:

- Who is "in charge" of CISR nationally, regionally, locally, and across the critical sectors?
- What are the key roles and responsibilities of the following with respect to CISR: FSLTT governments; industry; academia; research &development (R&D) entities; and nongovernmental organizations?
- How is each of the above players advantaged/disadvantaged regarding their individual CISR-related roles and responsibilities?
- What are the principal considerations and concerns in the CISR mission area across sectors and governmental jurisdictions?
- What are the key elements of the NIPP Partnership Model? How do the various government and private entities with CISR-related responsibilities at different levels under this model interact and collaborate with one another?
- How are the critical infrastructure sectors organized to accomplish the CISR mission at the sector and sub-sector levels? What is their "motivation" regarding their role in executing this mission?
- How does the distributed structure of responsibility and accountability play out against the principal threats we face in this mission area?
- What are the principal recommendations of the 2015 NIAC *Executive Collaboration for the Nation's Strategic Critical Infrastructure* Report? Do you concur with these recommendations?

3. In-class Activity. Learners will be organized into two-person teams. Each team will be assigned a specific sector to research with the objective of understanding the stakeholder landscape associated with the assigned sector. Learners should be prepared to discuss the following in the context of their assigned sectors:

- FSLTT agencies and private sector organizations that represent key sector stakeholders
- The principal authorities, roles, and responsibilities of each regarding CISR
- The main concerns and challenges faced by each

No formal presentation will be required. Additional Internet research will be needed.

4. Required Reading:

Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, pp. 10-12, Appendix B, 2013, http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.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.

National Infrastructure Advisory Council, *Executive Collaboration for the Nation's Strategic Critical Infrastructure*, Final Report and Recommendations, March 20, 2015, http://www.dhs.gov/sites/default/files/publications/niac-executive-collaboration-final-report-508.pdf

Peter R. Orszag, *Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentives*, Congressional Testimony, 2003, http://www.brookings.edu/~/media/Files/rc/testimonies/2003/0904healthcare_orszag/20030904.pdf.

Sue Eckert, *Protecting Critical Infrastructure: The Role of the Private Sector*, 2006, http://www.ridgway.pitt.edu/LinkClick.aspx?fileticket=Bezaq7AdjxA%3D&tabid=233.

Ken Schnepf, *Council Aims to Coordinate State/local Security Efforts*, 2007, http://www.plantservices.com/articles/2007/198.html.

The Role of ISACs in Private/Public Sector CIP,

2009, http://www.isaccouncil.org/images/ISAC_Role_in_CIP.pdf.

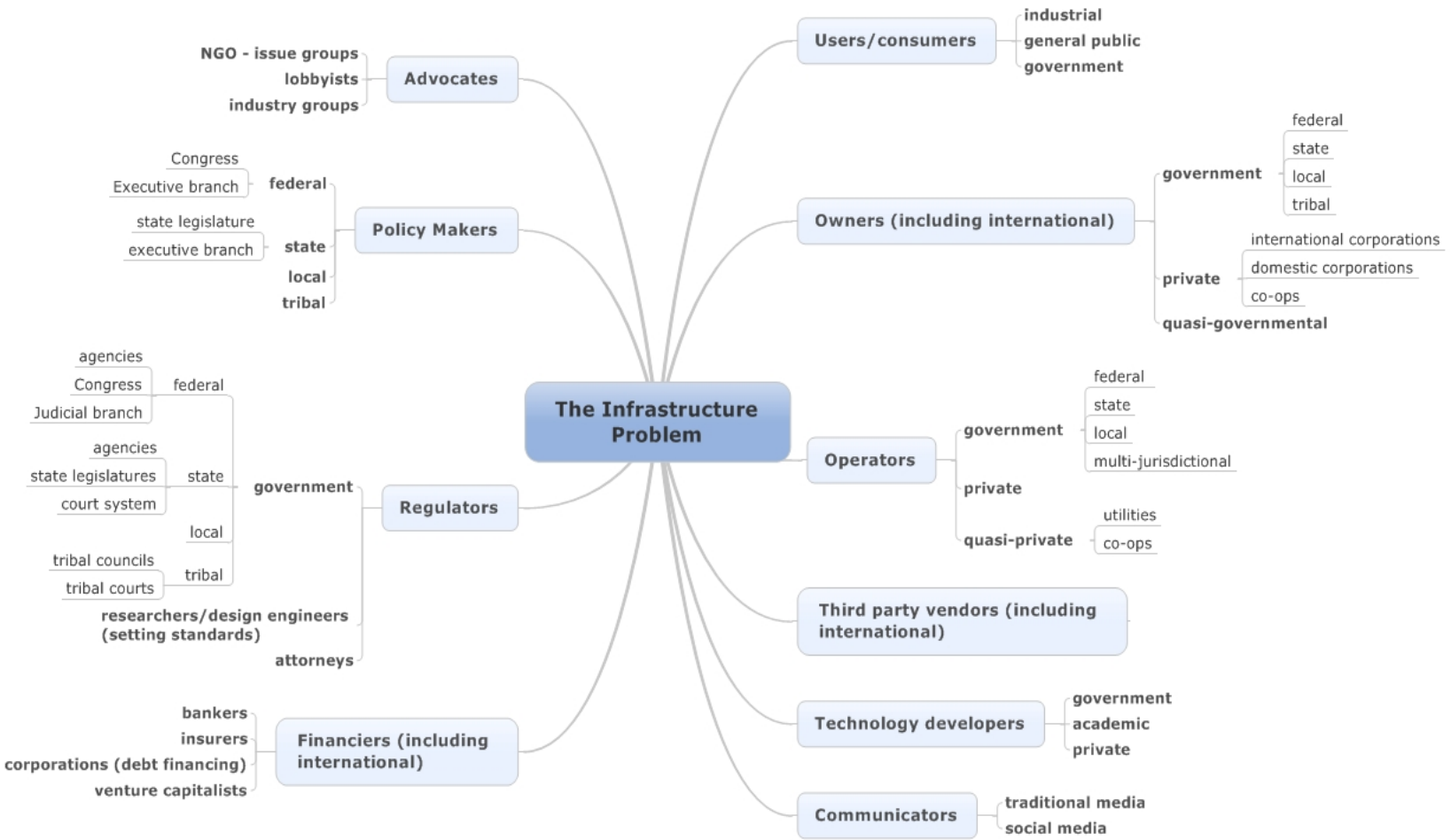
Foundations of Critical Infrastructure Security and Resilience

Lesson 4: Examining CISR Authorities, Roles, and Responsibilities: Federal, SLTT, and Private Sector

Lesson 4 Objectives

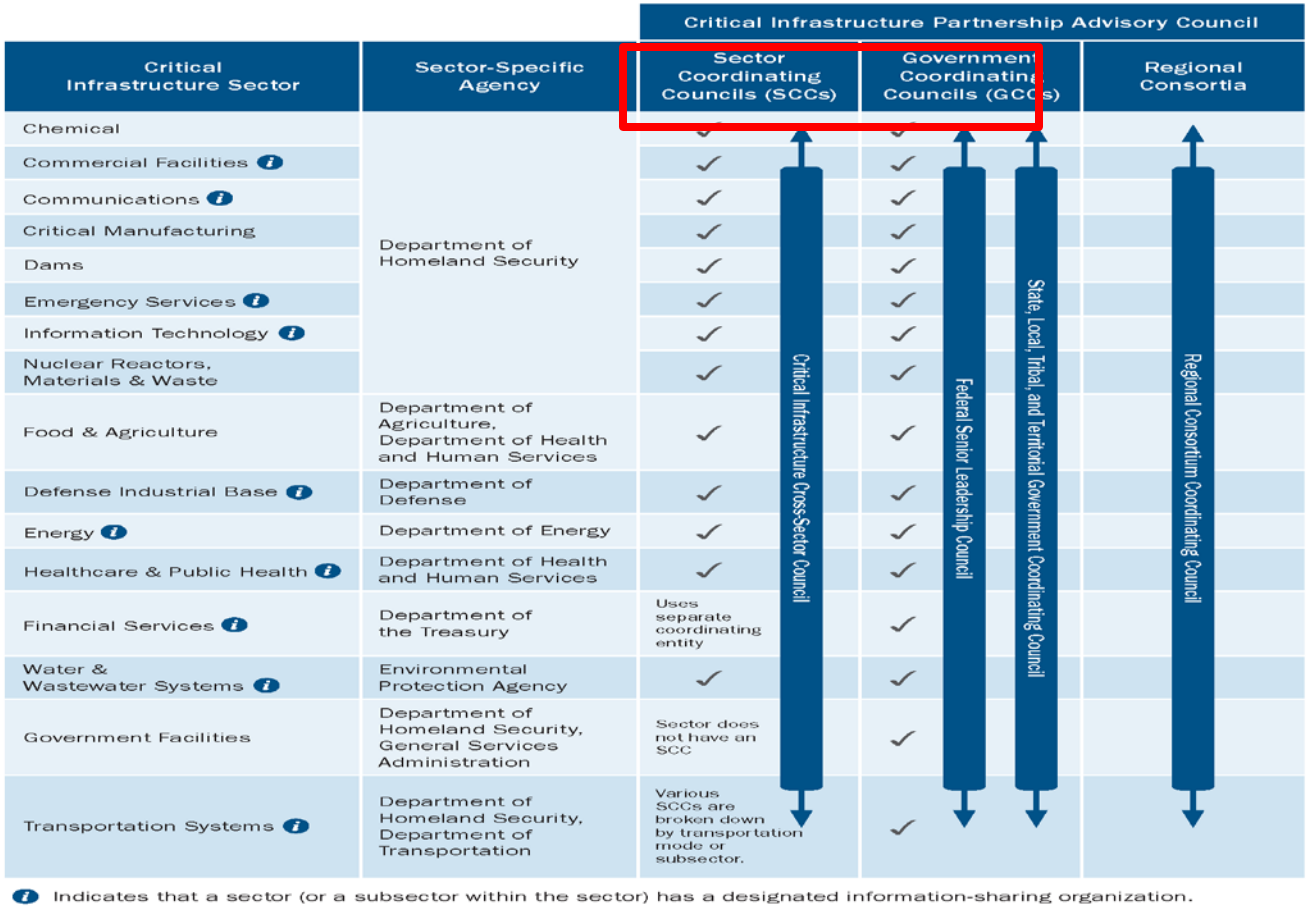
- Identify and describe the various public and private sector components of the NIPP Partnership Framework.
- Identify the various key stakeholders within the CISR mission space and discuss the authorities, roles, and responsibilities of each.
- Evaluate the principal political, organizational, legal, and resource challenges that those responsible for CISR face in executing those responsibilities.

The CISR Community: “Who Plays in the Space”



The NIPP Partnership Model

Sector and Cross-Sector Coordinating Structures



The NIPP Partnership Model

Public v. Private Sector Risk

PUBLIC SECTOR:
Accountable to the **TAXPAYER** using public funds

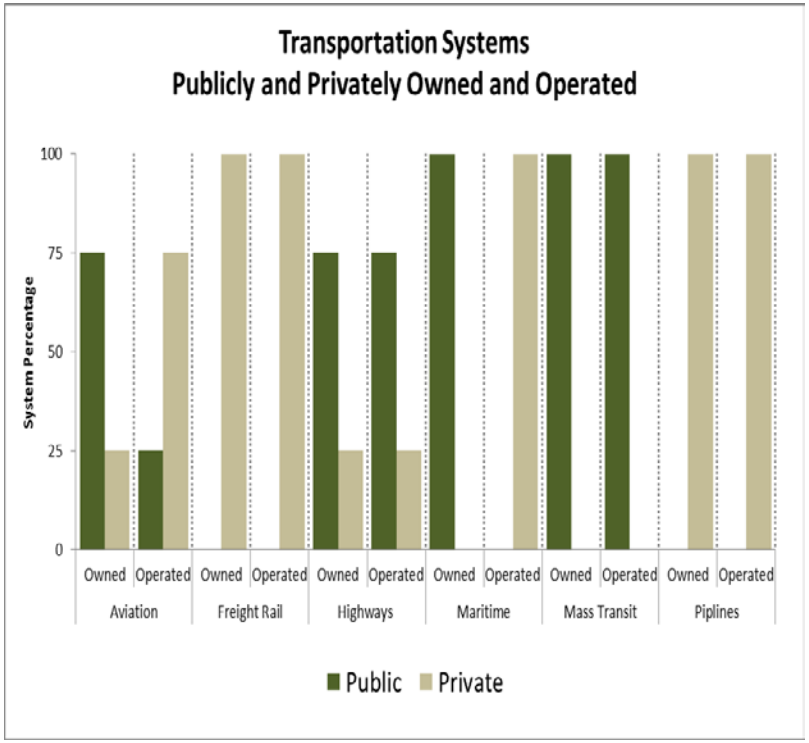
EXAMPLE: Roads, bridges, highways and port authorities

Governance: Boards, commissions and authorities, special purpose districts, local, State and Federal Governments

PRIVATE SECTOR:
Accountable to the **SHARE HOLDERS** using investors funds

EXAMPLE: Freight rail, port operators

Seven Class I railroads



12

The NIPP Partnership: Core Organizations

- Sector Coordinating Councils (SCCs)
- Critical Infrastructure Cross-Sector Council
- Government Coordinating Councils (GCCs)
- Federal Senior Leadership Council (FSLC)
- State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)
- Regional Consortium Coordinating Council (RC3)
- Information Sharing Organizations (Including ISACs)

Sector Coordinating Councils

- Self-organized, self-run, and self-governed councils that enable owners and operators, trade associations, vendors, and others to interact on a wide range of sector-specific strategies, policies, activities, and issues.
- Serve as policy coordination and planning entities to collaborate with SSAs/GCCs to address the entire range of sector CSIR activities and issues, serving as a voice for the sector and representing principal entry points for govn't collaboration.
- Serve as a strategic communication and coordination mechanism between owners, operators, suppliers, and the govn't during emerging threats and incidents.
- Identify, implement, and support appropriate info-sharing capabilities and mechanisms in sectors where no info-sharing structure exists.
- Facilitate inclusive organization and coordination of the sector's policy development regarding CSIR planning and preparedness, exercises and training, public awareness, and associated implementation activities and requirements.
- Identify, develop, and share info concerning effective cybersecurity practices.
- Provide input to the govn't on sector R&D efforts and requirements.

State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)

- Serves as a forum to promote engagement of SLTT partners as active participants in national CSIR efforts and provide an organizational structure to coordinate across jurisdictions on SLTT guidance, strategies, and programs.
- Provides senior-level, cross-jurisdictional strategic communications and coordination through partnership with the Federal Govn't and critical infrastructure owners and operators.
- Coordinates strategic issues and issue management resolution among Federal departments and agencies and SLTT partners.
- Coordinates with the FSLC, Critical Infrastructure Cross-Sector Council, and RC3 to support efforts to plan, implement, and execute the CSIR mission;
- Provides DHS info on SLTT-level security and resilience initiatives, activities, and best practices.
- Cooperates with DHS in establishing test sites for demonstration projects to support innovation.

PPD-21

- 3 Strategic Imperatives:
  - Refine/clarify “functional relationships” across the Federal govn’t & advance national unity of effort, including establishment of 2 national CI centers (physical & cyber)
  - Identify baseline info sharing data & systems requirements for Federal govn’t
  - Develop/implement a CI integration & analysis function to inform operational planning and strategic decisions (support SA & COP, prioritize assets, anticipate interdependencies/ cascading impacts, support incident management and recovery)

- Implementing Direction:
  - Develop report analyzing CI functional relationships/roles & responsibilities across Federal govn’t (including roles and functions of the two national CI centers and details on analysis and integration function)
  - Report evaluating existing public-private partnership model and making recommendations for improvement (physical and cyber)
  - Identify baseline data/systems requirements for the Federal govn’t to enable efficient info exchange
  - Develop real-time, all-hazards situational awareness capability for CI
  - Update NIPP and Nat’l CIPR R&D Plan

NIPP 2013 Call to Action

- **Call to Action #3: Empower Local and Regional Partnerships to Build Capacity Nationally**

- Local and regional partnerships contribute significantly to national efforts by increasing the reach of the national partnership, demonstrating its value, and advancing the national goals.

- Identify existing local and regional partnerships addressing CSIR, their alignment with national partnership structures, and how to engage with them.

- Leverage State and major urban area fusion centers to engage with local and regional partners.

- Expand a national network of CI and SLTT partnerships and coalitions to complement/enhance the national-level focus on sectors, while remaining cognizant of varying legal structures in different jurisdictions and organizations.

Discussion Questions: Partnerships

- How is CISR managed nationally, regionally, locally, and across the critical sectors?
- What are the key roles and responsibilities of the following with respect to CISR: Federal and SLTT governments; industry; academia; research &development (R&D) entities; and nongovernmental organizations?
- How is each of the above players advantaged/disadvantaged regarding their individual CISR-related roles and responsibilities?
- What are the principal considerations and concerns in the CISR mission area across sectors and governmental jurisdictions?
- What are the key elements of the NIPP Partnership Model? How do the various government and private entities with CISR-related responsibilities at different levels under this model interact and collaborate with one another?

Discussion Questions (Cont.)

- How are the critical infrastructure sectors organized to accomplish the CISR mission at the sector and sub-sector levels? What is their "motivation" regarding their role in executing this mission?

- How does the distributed structure of responsibility and accountability play out against the principal threats we face in this mission area?

- What are the principal recommendations of the 2015 NIAC *Executive Collaboration for the Nation's Strategic Critical Infrastructure* Report? Do you concur with these recommendations?

In-class Activity

- Learners will be organized into two-person teams. Each team will be assigned a specific sector to research with the objective of understanding the stakeholder landscape associated with the assigned sector. Learners should be prepared to discuss the following in the context of their assigned sectors:
  - FSLTT agencies and private sector organizations that represent key sector stakeholders.
  - The principal authorities, roles, and responsibilities of each regarding CISR.
  - The main concerns and challenges faced by each.