Lesson 8 Outline

Course Number: XXXX

Course: Foundations of Critical Infrastructure Security and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

LESSON 8 TOPIC: ENABLING CISR, MANAGING RISK, AND MEASURING PERFORMANCE: THE REGULATORY APPROACH

1. Lesson Goals/Objectives:

- Explain the strengths and weaknesses of the regulatory approach to CISR.
- Evaluate how risks are assessed and managed and how performance is measured in those sectors in which security, emergency preparedness, and emergency response are regulated by a government entity.
- Identify and discuss the differences in the approaches used in the regulated sectors: chemical/hazardous materials, freight rail, aviation, ports, commercial and nuclear facilities, electricity, and financial services.

2. Discussion Topics:

- What are the sectors in which security and other threat types are addressed in government regulations?
- What are the different approaches to regulation across the sectors? How does each address the major areas of risk assessment, management, and performance measurement?
- How do the regulators and regulated parties relate to one another in these individual approaches/models?
- What are the strengths and weaknesses of a regulatory approach to CISR?
- Do one or more models of regulation stand out as more effective than the others? If so, why?
- How do regulatory regimes deal with "outside-the-fence" security and emergency response concerns as well as critical dependency/interdependency issues?
- Is regulation working to produce a measurable increase in security or emergency preparedness in those sectors in which regulation is operative?

3. In-class Exercise: Learners will be divided into sector-specific discussion groups. Each group will be prepared to discuss and provide examples related to one of the NIPP Sector-Specific Plans (SSPs) in which CSIR primarily operates under a regulatory construct. Individual SSP reading assignments will be made by the instructor at the end of the previous lesson. The SSPs can be located at the following website: http://www.dhs.gov/critical-infrastructure-sectors.

4. Required Reading:

Lewis, Sector Specific Chapters (per in-class activity assignment)

Collins and Baggett, Chapters 6, 7, 9.

Public Law 107-295, *Maritime Transportation Security Act of 2002*, http://www.gpo.gov/fdsys/pkg/PLAW-107publ295/content-detail.html.

U.S. Department of Homeland Security, *Chemical Facility Antiterrorism Standards: Final*, 2007, http://www.dhs.gov/files/laws/gc_1166796969417.shtm.

Mark Holt and Anthony Andrew, *Nuclear Power Plants: Vulnerability to Terrorist Attack*, 2007, http://www.fas.org/sgp/crs/terror/RS21131.pdf.

Jack Spencer, "*U.S. Nuclear Policy after Fukushima: Trust but Modify*," Backgrounder No. 2557, The Heritage Foundation, 2011, http://thf_media.s3.amazonaws.com/2011/pdf/bg2557.pdf.

Paul Parfomak, *Pipeline Safety and Security: Federal Programs*, 2008, http://www.fas.org/sgp/crs/homesec/RL33347.pdf.

Security Spotlight, 2008, http://www.nrc.gov/security.html.

U.S. Government Accounting Office, *Freight Rail Security: Actions have been taken to Enhance Security, but the Federal Strategy can be Strengthened and Security Efforts Made Better*, 2009, http://www.gao.gov/new.items/d09243.pdf.

Electronic Code of Federal Regulation, *Rail Transportation Security*, 2009, http://www.gpo.gov/fdsys/pkg/FR-2009-05-20/pdf/E9-11736.pdf.

Committee to Review the Department of Homeland Security's Approach to Risk Analysis, National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis*, (2010), http://download.nap.edu/cart/deliver.cgi?record_id=12972.

George Mason University, The Center for Infrastructure Protection and Homeland Security (CIP/HS), *The CIP Report*, 10(3), September 2011, http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_September2011_9_11_10thAnniversary.pdf.

3. Additional Readings

Additional Readings (**See above for special instructions)**:
NIPP Sector Specific Plans (Chemical, Dams (Dam Safety), Energy (Electricity), Nuclear, Financial Services, Food and Agriculture (Food Safety and Biolab Security), Transportation Systems (Aviation, Maritime and Freight Rail), and Water and Wastewater Systems) located at http://www.dhs.gov/critical-infrastructure-sectors

George Mason University, The Center for Infrastructure Protection and Homeland Security, *Critical Infrastructure Protection: Elements of Risk,* Various articles, 2007, http://cip.gmu.edu/archive/archive/RiskMonograph_1207_rv.pdf.

Foundations of Critical Infrastructure Security and Resilience

Lesson 8: Enabling CISR, Managing Risk, and Measuring Performance: The Regulatory Approach

Lesson 8 Objectives

- Explain the strengths and weaknesses of the regulatory approach to CISR.
- Evaluate how risks are assessed and managed and how performance is measured in those sectors in which security, emergency preparedness, and emergency response are regulated by a government entity.
- Identify and discuss the differences in the approaches used in the regulated sectors: chemical/hazardous materials, freight rail, aviation, ports, commercial and nuclear facilities, electricity, and financial services.

Managing Critical Infrastructure Risk

- Key Factors in a regulatory construct
  - Authorities
  - Public-private interaction assessment, planning, information sharing, contingency response)
  - Dependencies/Interdependencies analysis
  - R&D/technological solutions
  - Resilient Design
  - Cybersecurity
  - Penalties vs. incentivization?

NIPP Risk Management Framework: How does this work in a regulatory framework?

- Physical, Cyber, and Human Elements of Risk
- Set Goals and Objectives
- Identify Infrastructure
- Assess and Analyze Risk
- Implement Risk Management Activities
  - Identify, Deter, Detect, Disrupt, and Prepare for Threats and Hazards
  - Reduce Vulnerabilities
  - Mitigate Consequences
- Measure Effectiveness

NIPP Risk Management Framework: How does this work in a regulatory framework?

- Nuclear Sector Example:
  - Commercial nuclear power plants regulated by the NRC (Security & Emergency Response) and FEMA (Community Preparedness)
  - "Outside-the-Fence" security is a function of collaboration between plant owners/operators, Fed law enforcement officials (FBI and USCG), SLTT law enforcement officials (including NG forces under State control), DHS Protective Security Advisors, etc.
  - "Outside-the Fence" emergency response is a function of collaboration between plant owners/operators, FEMA regional staff, SLTT emergency managers, DHS Protective Security Advisors, etc.

Result: CISR = multiple layers and levels of communication, coordination and collaboration inside and outside of regulated space.

In-Class Exercise

- Learners will be divided into sector-specific discussion groups. Each group will be prepared to discuss and provide examples related to one of the NIPP SSPs in which CISR operates under a regulatory construct.

Discussion Questions

- What are the sectors in which security and other threat types are addressed in government regulations?
- What are the different approaches to regulation across the sectors? How does each address the major areas of risk assessment, management, and performance measurement?
- How do the regulators and regulated parties relate to one another in these individual approaches/models?
- What are the strengths and weaknesses of a regulatory approach to CISR?

Discussion Questions (Cont.)

- Do one or more models of regulation stand out as more effective than the others? If so, why?
- How do regulatory regimes deal with “outside-the-fence” security and emergency response concerns as well as critical dependency/interdependency issues?
- Is regulation working to produce a measurable increase in security or emergency preparedness in those sectors in which regulation is operative?