Lesson 7 Outline

Course Number: XXXX

Course: Foundations of Critical Infrastructure Security and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

LESSON 7 TOPIC: ENABLING CISR, MANAGING RISK, AND MEASURING PERFORMANCE: THE VOLUNTARY APPROACH

1. Lesson Goals/Objectives:

- Explain the strengths and weaknesses of the various voluntary approaches to CISR across the various sectors.
- Evaluate how risks are assessed and managed and how performance is measured in those sectors in which security is not regulated by a government entity.
- Identify and discuss the various resources made available by the Federal government to other levels of government and the private sector to foster CISR program development and implementation.

2. Discussion Topics:

- What are the sectors in which security is not under government regulatory oversight? Which sectors use a hybrid voluntary-regulatory approach?
- What are the different approaches to voluntary security collaboration and coordination across the sectors? How does each address the major areas of risk assessment, management, and performance measurement?
- How does government at various levels relate to the private sector in these various sector level approaches/models?
- What are the strengths and weaknesses of a purely voluntary approach to CISR?
- Are there one or more models of voluntary security collaboration/coordination that stands out as more effective than the others? If so, why?
- How do voluntary security regimes deal with "outside-the-fence" security concerns as well as critical dependency/interdependency issues?
- Is the voluntary approach working to produce a measurable increase in security in those sectors in which regulation is not operative?
- What are the various resources made available by the Federal government to other levels of government and the private sector to foster CISR program development and implementation?

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 voluntary 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 8 and 9.

Philip Auerswald, Lewis M. Branscomb, Todd M. LaPorte and Erwann Michel-Kerjan, *The Challenge of Protecting Critical Infrastructure*, 2005, http://opim.wharton.upenn.edu/risk/downloads/05-11-EMK.pdf.
Bill Johnstone, *New Strategies to Protect America: Terrorism and Mass Transit after London and Madrid*, 2007, http://www.americanprogress.org/issues/security/news/2005/08/10/1592/new-strategies-to-protect-america-terrorism-and-mass-transit-after-london-and-madrid/

Claudia Copeland, *Terrorism and Security Issues Facing the Water Sector*, 2009, http://www.fas.org/sgp/crs/terror/RL32189.pdf.

U.S. Government Accountability Office, *Homeland Security: Actions Needed to Improve Response to Potential Terrorist Attacks and Natural Disasters Affecting Food and Agriculture*, August 2011, http://www.gao.gov/products/GAO-11-652

National Academy of Sciences, *Sustainable Critical Infrastructure Systems: A Framework for Meeting 21st Century Imperatives*, 2009, http://www.nap.edu/openbook.php?record_id=12638&page=R1.

Association of Corporate Counsel, *Superstorm Sandy foreshadows a new paradigm for protecting critical communications and electric infrastructure*, November 2012, http://www.lexology.com/library/detail.aspx?g=04ab535e-3535-465d-a41d-5605a6502833

Nessler, Clay, *Building Resilience – Six Lessons from Superstorm Sandy*, 2013, http://www.institutebe.com/smart-grid-smart-building/Building-Resilience.aspx

Gridwise Alliance, *Improving Electric Grid Reliability and Resilience: Lessons Learned from Superstorm Sandy and Other Extreme Events*, June 2013, https://www.naseo.org/Data/Sites/1/documents/committees/energysecurity/documents/gridwise-superstorm-sandy-workshop-report.pdf

Erickson, Mitchell, D., *A Bridge to Prosperity: Resilient Infrastructure Makes a Resilient Nation*, 2009, http://view.fdu.edu/files/brkprsericksonapr10.pdf

4. Additional Readings (**See above for special instructions)**:
NIPP Sector Specific Plans (Communications, Defense Industrial Base, Energy (Oil & Gas), Financial Services, Food and Agriculture, Information Technology, Transportation Systems, 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.

Daniel Prieto, *Mass Transit after the London Bombings*, 2005, http://belfercenter.ksg.harvard.edu/publication/3275/mass_transit_security_after_the_london_bombings.html?breadcrumb=%2Fexperts%2F812%2Fdaniel_b_prieto.

U.S. Government Accounting Office, *Surface Transportation Security: TSA Has Taken Action to Manage Risk, Improve Coordination, and Measure Performance, but Additional Actions Would Enhance Its Effort*, April 2010, http://www.gao.gov/new.items/d10650t.pdf.

Foundations of Critical Infrastructure Security and Resilience

Lesson 7: Enabling CISR, Managing Risk, and Measuring Performance: The Voluntary Approach

Lesson 7 Objectives

- Explain the strengths and weaknesses of the various voluntary approaches to CISR across the various sectors.
- Evaluate how risks are assessed and managed and how performance is measured in those sectors in which security is not regulated by a government entity.
- Identify and discuss the various resources made available by the Federal government to other levels of government and the private sector to foster CISR program development and implementation.

Managing Critical Infrastructure Risk

- Key Factors (Voluntary CISR approach)
  - Defining the value proposition
  - Leadership/governance/organization
  - Public-private cooperation & collaboration (risk assessment, planning, information sharing, contingency response)
  - Dependencies/Interdependencies analysis
  - R&D/technological solutions
  - Resilient Design
  - Cybersecurity
  - Incentivization

NIPP Risk Management Framework: How does this work under a voluntary paradigm?

- 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

Building Resilience in a Voluntary CISR Construct: Electricity Subsector Case Study

- Reduce the initial damage to building systems and infrastructure
- Improve the reliability of emergency back-up systems
- Have buildings support limited critical services for extended periods of time
- Designate and upgrade select buildings to provide critical community services
- Use passive design principles to increase building resilience
- Use distributed generation and micro-grids to increase community resilience

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 primarily operates under a voluntary construct.

Discussion Questions

- What are the sectors in which security is not under government regulatory oversight? Which sectors use a hybrid voluntary-regulatory approach?
- What are the different approaches to voluntary security collaboration and coordination across the sectors? How does each address the major areas of risk assessment, management, and performance measurement?
- How does government at various levels relate to the private sector in these various sector level approaches/models?
- What are the strengths and weaknesses of a purely voluntary approach to CISR?
- Are there one or more models of voluntary security collaboration/coordination that stands out as more effective than the others? If so, why?

Discussion Questions (Cont.)

- How do voluntary security regimes deal with “outside-the-fence” security concerns as well as critical dependency/interdependency issues?
- Is the voluntary approach working to produce a measurable increase in security in those sectors in which regulation is not operative?
- What are the various resources made available by the Federal government to other levels of government and the private sector to foster CISR program development and implementation?