Lesson 6 Outline

Course Number: XXXX

Course: Foundations of Critical Infrastructure Security and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

LESSON 6 TOPIC: ASSESSING CRITICAL INFRASTRUCTURE RISK IN AN INTERDEPENDENT WORLD

****Special Activity: Research paper topics must be submitted prior to class**

1. Lesson Goals/Objectives:

- Define the major elements of critical infrastructure risk in the context of its major components: threat, vulnerability, and consequence
- Critique the NIPP strategic risk management process, as well as how other government and private sector critical infrastructure stakeholders view and evaluate risk
- Explain how risk drives risk management strategies, plans, and resource investment across government and the private sector
- Explain how CISR-focused risk differs from that applied in the context of other disciplines (security, engineering, finance, business, etc.)
- Compare and contrast terrorism risk and the risk represented by natural disasters and other manmade hazards
- Evaluate the complexities regarding critical infrastructure dependencies and interdependencies as they relate to risk and its component elements

2. Discussion Topics:

- What are the major elements of risk as they pertain to the CISR mission? How are they quantified to support risk management decisions?
- How does the NIPP address the subject of risk and its component elements? How are risks prioritized within the NIPP framework?
- How do the human, physical, and cyber dimensions of CISR relate to the concept of risk?
- Does terrorism risk differ from the risk associated with natural disasters and other manmade hazards? If so, how?
- How does the Federal government assess risk and communicate the results of the risk assessment process to other CISR stakeholders? Do these other players have a role to play in government risk assessment processes and programs?
- How does risk management relate to strategic decisions and resource investments in the CISR mission area?
- How do we calculate risk across threat/hazard types? Across jurisdictions? Across sectors?

- Is there room for subjectivity in the risk analysis process?
- How does the issue of critical infrastructure dependencies/interdependencies complicate the risk assessment process? How do we measure these dependencies and interdependencies?
- Can we ever get to a completely risk-based CISR construct?
- Should we base the allocation of critical infrastructure-related grant funding on the notion of risk? Is the system working?

3. In-class Activities:

Activity 1: Learners will be divided into groups of 2 or 3 individuals. Each group will examine a risk assessment methodology currently in use in one of the critical infrastructure sectors and be prepared to discuss how the methodology works, as well as highlight the strengths and weaknesses of the methodology studied. Representative risk assessment methodologies include the following:

- **Threat and Hazard Identification and Risk Assessment (THIRA).** A guide for performing an all-hazards risk assessment provided by FEMA.
  Source:
  Threat and Hazard Identification and Risk Assessment Guide: Comprehensive Preparedness Guide (CPG) 201, Second Edition, 2013.

- **Chemical Facility Anti-Terrorism Standards (CFATS).** Regulations providing required security standards for identified high-risk chemical facilities.
  Sources:
  Risk-Based Performance Standards Guidance: Chemical Facility Anti-Terrorism Standards, Department of Homeland Security, May 2009.
  CSAT Top-Screen Survey Application: User Guide v. 1.99, Department of Homeland Security, September 2010.
  CSAT Security Vulnerability Assessment Application: Instructions v. 2.1, Department of Homeland Security, January 2011.

- **Critical Infrastructure Security Framework.** A framework developed by Sandia National Laboratories for performing risk assessments for critical infrastructure.
  Source:
  A Scalable Systems Approach for Critical Infrastructure Security, Sandia National Laboratories, SAND2002-0877, 2002.

- **Maritime Security Risk Analysis Model (MSRAM).** United States Coast Guard risk assessment.
  Source:
  Maritime Security Risk Analysis Model Overview for USCG-CREATE Maritime Risk Symposium, 2010.

- **Food and Agriculture Systems Criticality Assessment Tool.** Criticality assessment tool used by the Food and Agriculture Sector.
  Source:
  Huff et al., 2013. The Development and Use of the Food and Agriculture Systems

Criticality Assessment Tool (FASCAT). Food Protection Trends, Vol 33, No. 4, p. 218–223.

- **Infrastructure Survey Tool (IST).** Data collection tool used by DHS to calculate vulnerability, resilience, and criticality indices for critical infrastructure assets.
  Sources:
  Fisher, RE and Norman, M. Developing measurement indices to enhance protection and resilience critical infrastructure and key resources. Journal of Business Continuity & Emergency Planning, vol. 4 no. 3.
- Argonne National Laboratory, 2010. Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program.
  Argonne National Laboratory, 2009. Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program.

- **Vulnerability Self-Assessment Tool (VSAT).** Stand-alone model developed by the Environmental Protection Agency (EPA) for use by individual utilities in the Water Sector.
  Sources:
  VSAT Methodology Guide, 2014.
  Water Health and Economic Analysis Tool Model Documentation, 2014.

Activity 2: Learners will also be asked to come to class prepared to discuss key dependencies & interdependencies issues related to their sector of study in the context of real world situations.

4. Required Reading:
Collins and Baggett, Chapter 5.

Lewis, Chapters 2 & 4.

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, pp. 15-20,
http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf

http://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf

Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, *Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies*, 2004, http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.

Y.Y. Haimes, "Infrastructure Interdependencies and Homeland Security," *ASCE Journal of Infrastructure Systems*, 11(2), 2005, 65-66.
http://www.wou.edu/~koboldm/RCTP/RCTP%20Resource%20Handbook/Haimes_infrastructure_interdependencies_and_homeland_securit.pdf.

Congressional Research Service Report, *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options*, 2006, http://assets.opencrs.com/rpts/RL33206_20080912.pdf.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *Critical Infrastructure Protection: Elements of Risk*, Various articles, 2007, http://cip.gmu.edu/wp-content/uploads/2014/03/ElementsofRiskMonograph.pdf.

U.S. Government Accountability Office, *CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR RISK ASSESSMENTS: DHS Should Establish More Specific Guidance for Their Use*, 2012, http://www.gao.gov/assets/590/587674.pdf

U.S. Government Accountability Office, *Homeland Security: DHS Risk-based Grant Methodology is Reasonable, but Current Version's Measure of Vulnerability is Limited,"* 2008, http://www.gao.gov/new.items/d08852.pdf.

U.S. Government Accountability Office, *Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities*, 2011, http://www.gao.gov/new.items/d11537r.pdf.

George Mason University, Center for Infrastructure Protection and Homeland Security (CIP/HS), *The CIP Report*, 10(2), 2011, http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_August2011_Interdependencies.pdf.

Michel Van Eeten, Albert Nieuwenhuijs, Eric Luiijf, Marieke Klaver, and Edite Cruz, "The State and the Threat of Cascading Failure across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports," *Public Administration*, 89(2), 2011, 381–400, http://onlinelibrary.wiley.com/doi/10.1111/j.1467-9299.2011.01926.x/abstract.

5. Recommended Additional Reading:

U.S. Government Accountability Office, *Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security*, 2008, http://www.gao.gov/new.items/d08904t.pdf.

DHS, "Risk Lexicon," http://www.fema.gov/pdf/government/grant/2011/fy11_hsgp_lexicon.pdf.

Foundations of Critical Infrastructure Security and Resilience

Lesson 6: Assessing Critical Infrastructure Risk in an Interdependent World

Lesson 6 Objectives

- Define and discuss the major elements of critical infrastructure risk: threat, vulnerability, and consequence.
- Critique the NIPP strategic risk management process, as well as how other government and private sector critical infrastructure stakeholders view and evaluate risk.
- Explain how risk drives risk management strategies, plans, and resource investment across government and the private sector.
- Explain how CISR-focused risk differs from that applied in the context of other disciplines.

Lesson 6 Objectives (Cont.)

- Compare and contrast terrorism risk and the risk represented by natural disasters and other manmade hazards.

- Evaluate the complexities regarding critical infrastructure dependencies/interdependencies as they relate to risk.

Key Definitions

- **Critical infrastructure** represents “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

- PPD-21 defines **security** as “reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.”

Key Definitions(Cont.)

- **Consequence:** The effect of an event, incident, or occurrence. It reflects the level, duration, and nature of the loss resulting from the incident. Potential consequences may include public health and safety (i.e., loss of life and illness), economic (direct and indirect), psychological, and governance/mission impacts.

- **Vulnerability:** A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given threat or hazard. In calculating the risk of an intentional threat, a common measure of vulnerability is the likelihood that an attack is successful, given that it is attempted.

Key Definitions(Cont.)

- **Threat:** A natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. For the purpose of calculating risk, the threat of an unintentional hazard is generally estimated as the likelihood that a hazard will manifest itself. An intentional hazard is generally estimated as the likelihood of an attack being attempted by an adversary. In the case of intentional adversarial actors and actions, for both physical and cyber effects, the threat likelihood is estimated based on the intent and capability of the adversary.

NIPP Risk Management 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

Physical, Cyber, and Human Elements of Risk: HPH Sector Examples

- Human threats to the sector refer to the CI workforce, both as an asset that must be protected and a risk that could surface as a threat vector. Human threats to the sector encompass a wide array of potential threat actors ranging from disaffected employees to active shooters to domestic and international terrorist organizations.

- Physical facilities and assets comprising the HPH Sector include a geographically distributed array of physical assets and supporting infrastructure that can be impacted by a number of complex manmade and naturally occurring threats and hazards.

- In the context of cyber risk, the HPH Sector is increasingly dependent upon the secure storage and transmission of private data to dictate care, maintain patient records, safeguard intellectual property, and control financial operations.

NIPP Core Criteria for Risk Assessments

- **Key Points of the NIPP RMF:**
  - Risk, as defined by the NIPP RMF, is a function of consequence, vulnerability and threat.
  - Risk assessments should be based upon all 3 components of risk across their human, physical and cyber dimensions.
  - Risk assessments should be a function of scenario-based consequence and vulnerability estimates, and an assessment of the likelihood of specifically identified threats or hazards.
  - Risk assessment methodologies should be based on basic analytic principles to ensure they are properly documented, reproducible, and defensible.
- .

Core Criteria for Consequence Assessments

Core Criteria Guidance for Consequence Assessments
• Document the scenarios assessed, tools used, and any key assumptions made.
• Estimate the number of fatalities, injuries, and illnesses, where applicable and feasible, keeping each separate estimate visible to the user
• Estimate the economic loss in dollars, stating which costs are included
• If monetizing the human health consequences, document the value(s) used and the assumptions made
• Consider and document any protective or consequence mitigation measures that have their effect after the incident has occurred
• Describe psychological impacts and mission disruption, where feasible

Core Criteria for Vulnerability Assessments

Core Criteria Guidance for Vulnerability Assessments
• Identify the vulnerabilities associated with: physical, cyber, or human factors; critical dependencies; and physical proximity to hazards
• Describe all protective measures in place and how they reduce the vulnerability for each scenario
• In evaluating security vulnerabilities, develop estimates of the likelihood of an adversary's success for each attack scenario
• For natural hazards, estimate the likelihood that an incident would cause harm to the asset, system or network, given that the natural hazard events occurs at the local of interest for the risk scenario

Core Criteria for Threat Assessments

Core Criteria Guidance for Threat Assessments
For adversary-specific threat assessments:
• Account for the adversary's ability to recognize the target and the deterrence value of existing security measures
• Identify attack methods that may be employed
• Consider the level of capability that an adversary demonstrates with regard to a particular attack method
• Consider the degree of the adversary's intent to attack the target
• Estimate threat as the likelihood that an adversary would attempt a given attack method against the target
• If threat likelihoods cannot be estimated, use conditional risk values (consequence times vulnerability) and conduct sensitivity analyses to determine how likely the scenario would have to be to support the decision
For natural disasters and accidental hazards:
• Use best-available analytic tools and historical data to estimate the likelihood that these events would affect CI.

Example Threat Assessment Matrix

Threat Evaluation Matrix					
Threat Level	Existence	Capability	History	Intentions	Targeting
Critical	●	●	●	●	●
High	●	●	●	●	○
Medium	●	●	●	○	○
Low	●	●	○	○	○
Negligible	○	○	○	○	○

● = Factor must be present
○ = Factor may or may not be present

CI Dependencies & Interdependencies

- Our nation's critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies.

- *Dependency:* A linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other.
  - Electric power infrastructure requires natural gas and petroleum fuels for its generators, road and rail transportation and pipelines to supply fuels to the generators, air transportation for aerial inspection of transmission lines, water for cooling and emissions control, and telecommunications for e-commerce and for monitoring system status and system control and energy management systems.

- *Interdependency:* A bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other.

CI Dependencies & Interdependencies (Cont.)

- 4 principal classes of interdependencies: *physical, cyber, geographic, and logical.*
  - Two infrastructures are physically interdependent if the state of each is dependent on the material output(s) of the other.
  - An infrastructure has a cyber interdependency if its state depends on information transmitted through the information infrastructure.
  - Infrastructures are geographically interdependent if a local environmental event can create state changes in all of them.
  - Two infrastructures are logically interdependent if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection.
- Interdependencies increase the risk of failures or disruptions in multiple infrastructures.
- A *cascading failure* occurs when a disruption in one infrastructure causes the failure of a component in a second infrastructure, which subsequently causes a disruption in the second infrastructure.

In-Class Activities

- Learners will be divided into groups of 2 or 3 individuals. Each group will examine a risk assessment methodology currently in use in one of the critical infrastructure sectors and be prepared to discuss how the methodology works, as well as highlight the strengths and weaknesses of the methodology studied.

- Learners will also discuss key dependencies & interdependencies issues related to their sector of study in the context of past real world all-hazards incidents.

Discussion Questions

- What are the major elements of risk as they pertain to the CISR mission? How are they quantified to support risk management decisions?
- How does the NIPP address the subject of risk and its component elements? How are risks prioritized within the NIPP framework?
- How do the human, physical, and cyber dimensions of CISR relate to the concept of risk?
- Does terrorism risk differ from the risk associated with natural disasters and other manmade hazards? If so, how?
- How does the Federal government assess risk and communicate the results of the risk assessment process to other CISR stakeholders? Do these other players have a role to play in government risk assessment processes and programs?

Discussion Questions (Cont.)

- How does risk management relate to strategic decisions and resource investments in the CISR mission area?
- How do we calculate risk across threat/hazard types? Across jurisdictions? Across sectors?
- Is there room for subjectivity in the risk analysis process?
- How does the issue of critical infrastructure dependencies/interdependencies complicate the risk assessment process? How do we measure these dependencies and interdependencies?
- Can we ever get to a completely risk-based CISR construct?
- Should we base the allocation of critical infrastructure-related grant funding on the notion of risk? Is the system working?