Lesson 2 Outline

Course Number: XXXX

Course: Foundations of Critical Infrastructure Security and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

LESSON 2 TOPIC: DEFINING AND ACHIEVING CRITICAL INFRASTRUCTURE RESILIENCE

1. Lesson Goals/Objectives:

- Explain the concept of "resilience" and its application to the CISR mission area.
- Understand the general principles associated with resilience as currently applied within government and industry in the U.S. context.
- Discuss the similarities and differences between operational resilience, community resilience, organizational resilience, and personal resilience.
- Identify and evaluate various strategies and initiatives currently underway to enhance critical infrastructure resilience across all levels of government and the private sector.

2. Discussion Topics:

- What is the concept of "resilience" as it applies to the CISR mission area?
- How do PPD-8, PPD-21, and the NIPP 2013 define "resilience" for critical infrastructure? How does resilience relate to the various aspects of the National Preparedness System?
- What does "resilience" mean in the context of specific types of manmade and naturally occurring threats and hazards?
- Are "security" and "resilience" mutually exclusive concepts?
- What are the general principles associated with resilience as currently applied within government and industry in the U.S.?
- How do we make our critical infrastructure more resilient? What are the drivers for doing so? What are the impediments to doing so?
- Discuss the similarities and differences between operational resilience, community resilience, organizational resilience, and personal resilience. How are they related? How are they different?
- What are the various approaches being used to operationalize critical infrastructure resilience at a regional and sub-regional level in the U.S.?
- What are the major recommendations of the 2009 and 2013 National Infrastructure Advisory Council (NIAC) Reports regarding resilience? Do you concur with them? If not, what would be your recommendations?
- How can resilience and resilience-focused investments be measured within and

across the critical infrastructure sectors?

3. **In-Class Activity:** Learners will be divided into groups to independently identify and discuss the core elements of an overarching framework for achieving critical infrastructure resilience within one of the critical infrastructure sectors (pre-assigned by the instructor). The breakout groups will reconvene in plenary session to walk through their respective observations and conclusions.

4. Required Reading:

Brandon J. Hardenbrook, *The Need for a Policy Framework to Develop Disaster Resilient Regions*, 2005, http://www.degruyter.com/view/j/jhsem.2005.2.3/jhsem.2005.2.3.1133/jhsem.2005.2.3.1133.xml.

Dr. Jim Kennedy, *Critical Infrastructure Protection is all about Operational Resilience*, 2006, http://www.continuitycentral.com/feature0413.htm.

T.D. O'Rourke, *Critical Infrastructure, Interdependencies and Resilience*, Spring 2007, http://www.nae.edu/File.aspx?id=7405.

Brian Jackson, *Marrying Prevention and Resiliency*, 2008, http://www.rand.org/pubs/occasional_papers/2008/RAND_OP236.pdf.

National Infrastructure Advisory Council, *Critical Infrastructure Resilience Final Report and Recommendations*, September 2009, http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

National Infrastructure Advisory Council, *Optimization of Resources for Mitigation of Infrastructure Disruption Study Final Report and Recommendations*, October 19, 2010, http://www.dhs.gov/xlibrary/assets/niac/niac-optimization-resources-final-report-10192010.pdf.

The Infrastructure Security Partnership, *Understanding Resilience: Disaster Resilience Begins with You*, July 30, 2013, http://www.tisp.org/index.cfm?cdid=13180&pid=10261.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 12(6), December 2013, http://cip.gmu.edu/wp-content/uploads/2014/01/December-2013_Resilience.pdf.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 12(7), January 2014, http://cip.gmu.edu/wp-content/uploads/2013/06/January-2014_Resilience.pdf.

Foundations of Critical Infrastructure Security and Resilience

Lesson 2: Defining and Achieving Critical Infrastructure Resilience

Lesson 2 Objectives

- Explain the concept of “resilience” and its application to the CISR mission area.
- Understand the general principles associated with resilience as currently applied within government and industry in the U.S. context.
- Discuss the similarities and differences between operational resilience, community resilience, organizational resilience, and personal resilience.
- Identify and evaluate various strategies and initiatives currently underway to enhance critical infrastructure resilience across all levels of government and the private sector.

Critical Infrastructure Resilience

- Resilience is defined in *Webster's Unabridged Dictionary* as "the ability to bounce or spring back into shape, position, etc., after being pressed or stretched."

- PPD-21 defines **resilience** as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions...[it] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."
  - *Robustness*: the inherent strength or resistance in a system to withstand external demands without degradation or loss of functionality.
  - *Redundancy*: system properties that allow for alternate options, choices, and substitutions under stress.
  - *Resourcefulness*: the capacity to mobilize needed resources and services in emergencies.
  - *Rapidity*: the speed with which disruption can be overcome and safety, services, and financial stability restored.

Critical Infrastructure Resilience: Core Element Examples

- Robustness: Building codes and construction procedures for new and retrofitted structures; Emergency operations planning; Community preparedness; Regional economic diversification
- Redundancy: Capacity for technical substitutions and “workarounds;” Alternate sites for managing disaster operations; Ability to substitute and conserve needed inputs
- Resourcefulness: Availability of equipment and materials for restoration and repair; Capacity to improvise, innovate, and expand operations
- Rapidity: System downtime, restoration time; Time between impact and early recovery; Time to restore lifeline services; Time to regain capacity, lost revenue

PPD-8 & Resilience: How do they fit together?

- National Preparedness Goal
- National Preparedness System
- National Mission Area Frameworks
  - Prevention
  - Protection
  - Response
  - Recovery
  - Mitigation
- Federal Interagency Operational Plans
- How does “resilience” fit into the PPD-8 schemata?

NIPP 2013 Call to Action – Building Resilience?

- Set National Focus through Jointly Developed Priorities
- Determine Collective Actions through Joint Planning Efforts
- Empower Local and Regional Partnerships to Build Capacity Nationally
- Leverage Incentives to Advance Security and Resilience
- Enable Risk-Informed Decision Making through Enhanced Situational Awareness
- Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects
- Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents

NIPP 2013 Call to Action Review (Cont.)

- Promote Infrastructure, Community, and Regional Recovery Following Incidents
- Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education
- Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions
- Evaluate Progress toward the Achievement of Goals
- Learn and Adapt During and After Exercises and Incidents

Joint National Priorities – Building Resilience?

- Strengthen the Management of Cyber and Physical Risks to Critical Infrastructure
- Build Capabilities and Coordination for Enhanced Incident Response and Recovery
- Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines
- Enhance Effectiveness in Resilience Decision-Making
- Share Information To Improve Prevention, Protection, Mitigation, Response, and Recovery Activities

Resilience & Catastrophic Disasters: Planning Factors

- Enormity of consequences – speed of cascading infrastructure failure and “strategic surprise”
- Large-scale power outages, near total communications outages, massive transportation nodal/system disruptions
- Vulnerability of “clustered infrastructure”
- Multiple “disasters w/in a disaster”
- Massive evacuations & population displacement
- Crisis of public confidence likely – law & order?
- Social media is ubiquitous
- Traditional response capabilities acutely overwhelmed

Key Resilience-focused Lessons Learned from Recent Disasters

- Strong public-private partnerships accelerate response
- Senior executive-level engagement removes critical barriers
- Increasing interdependencies harbor hidden risks
- Lifeline sector service restoration needs are critical and not fully understood
- Large-scale events reveal critical points of failure and risks of aging infrastructure

Key Resilience-focused Lessons Learned from Recent Disasters (cont.)

- Co-location of key partners improves coordination and decision-making
- Joint regional exercises build response muscle memory
- Strong communities reduce impacts and improve recovery
- Complex rules, regulations, and processes hinder lifeline sector response
- Innovative social media use can revolutionize response
- Business case for infrastructure investment is difficult to define
- Risk data is needed to build stronger and redefine best practices

Building Critical Infrastructure Resilience for Catastrophic Disasters

- 3 overall objectives of building resilience:
  - 1) minimizing damage to critical infrastructure during the event
  - 2) maintaining operational integrity and critical services immediately following the event
  - 3) returning to normal, safe operating conditions as soon as possible

2013 NIAC Report on Strengthening Regional Resilience

- Three general principles:
  - Resilience requires a whole-of-nation approach that integrates top-down policy and leadership with bottom-up community capability to withstand and survive disasters.
  - Regional resilience strategies must be tailored to the distinct needs of each region and designed to manage complex regional risks that span multiple jurisdictions and sectors.
  - Strong public-private partnerships and relationships that include senior executive involvement are the most effective and enduring strategy for achieving sustainable resilience.

2013 NIAC Report on Strengthening Regional Resilience Recommendations

- Form partnerships with senior executives from the lifeline sectors, based on the Federal govnt's successful executive engagement with the electricity sector.

- Identify/develop regional, public-private, cross-sector partnerships, led by senior executives, to coordinate lifeline sector resilience efforts w/in a given region.

- Designate energy, communications, water, and transportation sectors as lifeline sectors and direct all agencies to recognize the priority of the lifeline sectors and the individuality of regions.

2013 NIAC Report on Strengthening Regional Resilience Recommendations (cont.)

- Integrate social media into public alert and warning systems and work with state and local government partners to develop social media information sharing capabilities to inform response.

- Launch a cross-agency team to develop solutions to site access, waiver, and permit barriers during disaster response.

- Create a strong value proposition for investment in resilient lifeline infrastructures and accelerate the adoption of innovative technologies in major infrastructure projects.

In-Class Exercise

- Learners will be divided into groups to independently identify and discuss the core elements of an overarching framework for achieving critical infrastructure resilience within one of the critical infrastructure sectors. The breakout groups will reconvene in a plenary session to walk through their respective observations and conclusions. The discussion will also include a mapping of the resilience framework developed by the learners against the the “Calls to Action” identified in the NIPP 2013 and corresponding “Joint National Priorities.”

Discussion Questions

- What is the concept of “resilience” as it applies to the CISR mission area?
- How do PPD-8, PPD-21, and the NIPP 2013 define “resilience” for critical infrastructure? How does “resilience” align to the various aspects of the National Preparedness System?
- What does “resilience” mean in the context of specific types of manmade and naturally occurring threats and hazards?
- Are “security” and “resilience” mutually exclusive concepts?
- What are the general principles associated with resilience as currently applied within government and industry in the U.S.?
- How do we make our critical infrastructure more resilient? What are the drivers for doing so? What are the impediments to doing so?

Discussion Questions (Cont.)

- Discuss the similarities and differences between operational resilience, community resilience, organizational resilience, and personal resilience. How are they related? How are they different?
- What are the various approaches being used to operationalize critical infrastructure resilience at a regional and sub-regional level in the U.S.?
- What are the major recommendations of the 2009 National Infrastructure Advisory Council (NIAC) Report regarding resilience? Do you concur with them? If not, what would be your recommendations?
- How can resilience and resilience-focused investments be measured within and across the critical infrastructure sectors?