Lesson 1 Outline

Course Number: XXXX

Course: XXXX

University of XXXXXX

Fall/Spring Semester 20XX

LESSON 1 TOPIC: INTRODUCTION TO CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

1. Lesson Goals/Objectives:

- Review the scope and objectives of the course, administrative requirements, instructional methodology, evaluation criteria, and feedback processes.
- Define and discuss the various interpretations of the term "critical infrastructure."
- Recognize CISR as a multidisciplinary field and the challenges this creates.
- Review and demonstrate an understanding of the various statutory and policy authorities that underpin the CISR mission area at the national level.
- Discuss and understand how CISR policy has evolved as a function of the all-hazards risk environment and other factors over time.

2. Discussion Topics:

- What is "critical infrastructure" and why is it important to us? How has the definition of critical infrastructure evolved over time?
- What are the general principles we typically associate with CISR in the U.S. context? How are these woven into strategy and policy at the national level?
- How have the CISR mission area and related national policy evolved over time from a historical perspective?
- What are the differences between, and the strengths and weaknesses of, the various Presidential policies focused on CSIR over the years?
- How has the U.S. approach to CISR been informed by the consequences of and response to specific natural and manmade threat/hazard situations?
- What are the principal advancements associated with the current U.S. national policy in this area: Presidential Policy Directive 8 (PPD-8), PPD-21, Executive Order (EO) 13636, and the NIPP 2013?) How are these various policy drivers interrelated?
- What are the major "Calls to Action" as presented in the NIPP 2013? What are the Joint National Priorities developed and issued by DHS and its NIPP partners? How might these Calls to Action/Joint National Priorities best be organized and implemented?
- How do CISR considerations factor into the National Preparedness Goal? The National Preparedness System? The "Whole Community" approach?
- What does the Homeland Security Act of 2002 have to say about "infrastructure

protection?" How does the U.S. Congress view the CISR mission area? Does legislation (i.e. regulation) clarify or complicate the CISR mission space?

- Where should the next Administration/Congress take the CISR mission area?

3. In-Class Activity. Learners will be divided into groups to critique the various "Calls to Action" identified in the NIPP 2013 and corresponding "Joint National Priorities" and discuss how they might be further be defined, refined, and implemented through the NIPP public-private partnership.

4. Required Reading:
Lewis, Chapter 1.

Collins and Baggett, Chapters 1-3.

Brown, Chapters 1-4, 8, and 9.

John D. Moteff, *Critical Infrastructure Protection: Background, Policy and Implementation*, 2014, http://www.fas.org/sgp/crs/homesec/RL30153.pdf.

Presidential Decision Directive-63, Critical Infrastructure Protection, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

Homeland Security Act of 2002, PUBLIC LAW 107–296—NOV. 25, 2002, Sections 201-215, https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

Homeland Security Presidential Directive-7,
Critical Infrastructure Identification, Prioritization and Protection,
(2003), http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1.

Presidential Policy Directive-8, National Preparedness, (2011), http://www.dhs.gov/presidential-policy-directive-8-national-preparedness.

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.

Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 12, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, pp. 1-10, 13-14, http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf.

U.S. Department of Homeland Security, *Joint National Priorities for Critical*

Infrastructure Security and Resilience, (2014), *http://www.dhs.gov/sites/default/files/publications/JointNationalPrioritiesFactSheet-508.pdf*

Congressional Research Service Report, *Critical Infrastructure Resilience: The Evolution of Policies and Programs and Issues for Congress*, (August 23, 2012), http://www.fas.org/sgp/crs/homesec/R42683.pdf

5. Additional Recommended Reading:

Clark Staten. *Reflections on the 1997 Commission on Critical Infrastructure Protection Report.* 1997. http://www.blythe.org/nytransfer-subs/97cov/PCCIP;_Critical_Infrastructure_Protection_Report.

The 9/11 Commission Report, *Final Report of the National Commission on Terrorist Attacks Upon the United States*, Chapters 2, 3, 6 and 7, 2004 http://www.9-11commission.gov/.

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. 2003. http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

U.S. Department of Homeland Security, *National Preparedness Goal*, (2011), http://www.fema.gov/media-library-data/20130726-1828-25045-9470/national_preparedness_goal_2011.pdf.

U.S. Department of Homeland Security, *National Preparedness System*, (2011), http://www.fema.gov/media-library-data/20130726-1855-25045-8110/national_preparedness_system_final.pdf.

U.S. Department of Homeland Security, *Quadrennial Homeland Security Review, 2014*, http://www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.pdf.

Foundations of Critical Infrastructure Security and Resilience

Lesson 1: Introduction to Critical Infrastructure Security and Resilience

Lesson 1 Objectives

- Review the scope and objectives of the course, administrative requirements, instructional methodology, evaluation criteria, and feedback processes.

- Define and discuss the various interpretations of the term “critical infrastructure.”

- Recognize CISR as a multidisciplinary field and the challenges this creates.

- Review and demonstrate an understanding of the various statutory and policy authorities that underpin the CISR mission area at the national level.

- Discuss and understand how CISR policy has evolved as a function of the all-hazards risk environment and other factors over time.

Course Overview

- Course Description
- Objectives
- Delivery Method
- Grading
- Major Course Activities and Requirements
  - Classroom Participation
  - Research Paper & Oral Presentation
  - Incident Management Exercise & Point Paper
- Course Readings
- Other Information

Course Outcomes/Objectives

- Understand the CISR policy, risk, and operational environments
- Understand key stakeholder authorities and responsibilities, partnership frameworks, information sharing processes/systems, and challenges related to all
- Assess the evolving 21st century risk environment and its implications for the CISR mission area
- Understand different approaches to CISR risk management, both regulatory and non-regulatory
- Develop practical familiarity with national incident management as it pertains to CISR
- Postulate future threats, challenges, and potential solutions

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.”

- 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.”

Strategic Context for Infrastructure Security & Resilience (1 of 2)

- **Dynamic threat/hazard environment**
  - Nation-states (rogue & otherwise)
  - Terrorists
  - Other Violent Extremists
  - Malicious Insiders
  - Catastrophic Natural Disasters
  - Technology Failures / Industrial Accidents / HAZMAT Releases
  - Cyber Attacks
  - Pandemics
  - Climate Change
  - Space Weather
  - Global Supply Chain Disruptions
  - WMD

Strategic Context for CISR (2 of 2)

- **Today's point of departure: a complex problem, requiring a national/regional/international approach and organizing framework**
  - 16 Sectors, all different, ranging from asset-focused to systems & networks
  - Inherent & increasing vulnerabilities, dependencies and interdependencies
  - Information sharing is still a big issue
  - Security/resilience are generally outside regulatory space (occupational & environmental safety are different matters) – with some notable exceptions
  - Shared responsibility and accountability at all levels; distributed authorities; no single entity "owns the problem;" "Whole Community" approach?
  - 85% privately owned; 100% located in State and local jurisdictions
  - Increasingly important international supply chain considerations
  - Security strategies must be tailored according to risk environment, operating landscapes and authorities/resources dynamics—human lives at risk vice denial of service focus
  - Resilience as a baseline; risk-based security layered on where appropriate
  - Actions must take into account "steady state" posture (sustainability) as well as emergent threats
  - Foreign ownership of U.S. infrastructure and cyber penetration are growing concerns

Managing Critical Infrastructure Risk

- Key Factors
  - Defining the value proposition
  - Leadership/governance
  - Public-private cooperation & collaboration (risk assessment, planning, contingency response)
  - International cooperation & collaboration
  - Cybersecurity
  - Interdependencies analysis
  - R&D/technological solutions
  - Infrastructure recapitalization
  - Regulatory vs voluntary solutions
  - Incentivization

Policy Evolution

- WWII – Cold War
- President’s Commission on CIP
- PPD-63
- 9/11 Attacks
- Physical and Cyber Strategies
- HSPD-7
- Hurricanes Katrina, Wilma and Rita
- NIPP 2006/2009
- PPD-8, PPD-21, EO 13636, EO 13691 and the NIPP 2013

PPD-8

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

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

Executive Order – Improving Critical Infrastructure Cybersecurity

- Policy: Increase volume, timeliness, and quality of cyber threat info shared w/ U.S. private sector entities so that they may better protect themselves against cyber threats.
  - AG, DHS Sec and DNI to ensure timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity…and develop process to rapidly disseminate reports to targeted entity. Process also to include dissemination of classified reports to CI entities authorized to receive them.
  - DHS Sec in collaboration with SECDEF to establish procedures expanding Enhanced Cybersecurity Services program to all CI sectors to provide classified cyber threat/technical info from Govn't to eligible CI companies or commercial service providers offering security services to CI entities.
  - DHS Sec to expedite processing of security clearances for appropriate personnel employed by CI owners/operators, and expand use of programs bringing private sector SMEs into Federal service on a temporary basis.
  - Commerce Sec to lead development of voluntary cybersecurity framework, including standards, methodologies, procedures, and processes to align policy, business, and technological approaches to address cyber risks to CI.
  - Sec DHS, in coordination with SSAs, to establish voluntary program to support adoption of Cybersecurity Framework, including incentives for doing so.
  - Sec DHS to identify CI where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health/safety, economic security, or national security.

NIPP 2013

- Mission: Strengthen the security and resilience of the Nation’s critical infrastructure by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure community.

- Goals:
  - Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities;
  - Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;
  - Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, as well as effective responses to save lives and ensure the rapid recovery of essential services;
  - Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and
  - Promote learning and adaption during and after exercises and incidents.

NIPP 2013: Call to Action

- 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 (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 (Iteration 1)

- 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

In-Class Exercise

- Learners will be divided into groups to critique the various “Calls to Action” identified in the NIPP 2013 and corresponding “Joint National Priorities” and discuss how they might be further defined, refined, and implemented through the NIPP public-private partnership.

Discussion Questions

- What is “critical infrastructure” and why is it important to us? How has the definition of critical infrastructure evolved over time?

- What are the general principles we typically associate with CISR in the U.S. context? How are these woven into strategy and policy at the national level?

- How have the CISR mission area and related national policy evolved over time from a historical perspective?

- What are the differences between, and the strengths and weaknesses of, the various Presidential policies focused on CSIR over the years?

- How has the U.S. approach to CISR been informed by the consequences of and response to specific natural and manmade threat/hazard situations?

- What are the principal advancements associated with the current U.S. national policy in this area: Homeland Security Act of 2002, Presidential Policy Directive 8 (PPD-8), PPD-21, Executive Order (EO) 13636, and the NIPP 2013? How are these various policy drivers interrelated?

Discussion Questions (Cont.)

- What are the “Calls to Action” as presented in the NIPP 2013? What are the Joint National Priorities developed and issued by DHS and its NIPP partners? How might these Calls to Action/Joint National Priorities best be organized and implemented?

- How do CISR considerations factor into the National Preparedness Goal? The National Preparedness System? The “Whole Community” approach?

- How does the U.S. Congress view the CISR mission area? Does legislation (i.e. regulation) clarify or complicate the CISR mission space?

- Where should the next Administration/Congress take the CISR mission area?