Lesson 3 Outline

Course Number: XXXX

Course: Foundations of Critical Infrastructure Security and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

LESSON 3 TOPIC: EXAMINING CISR IN THE CONTEXT OF THE 21ST CENTURY THREAT ENVIRONMENT

1. Lesson Goals/Objectives:

- Identify and evaluate the various threats and hazards that may impact critical infrastructure within and across the different sectors, and how they can be viewed in an all-hazards risk management approach.
- Explain the major elements of the Strategic National Risk Assessment (SNRA) and the Threat and Hazard Identification and Risk Assessment (THIRA) process, as well as their applicability to the CISR mission area.
- Discuss how the results of the THIRA process can be used to inform investments and capability delivery in the CISR mission area.
- Assess the challenges associated with achieving CISR in the current and projected threat environment.

2. Discussion Topics:

- Currently, what are the principal threats and hazards to our critical infrastructure assets, systems, and networks? At a sector level?
- How have these threats/hazards evolved over time in terms of potential impacts (magnitude and type)?
- Why would government expand its view of critical infrastructure to encompass targets that have amplifying effects, such as commercial facilities?
- What are the trends regarding international and domestic terrorist acts focused on critical infrastructure assets, systems, and networks?
- What part do our critical infrastructure "target sets" play in the concept of "asymmetric warfare?"
- What are "Essential Elements of Information" (EEIs) in the context of recognizing and addressing threats to CSIR? How are EEIs formulated, and what role do they play in an emergent threat or incident situation?
- What is the underlying analytical approach underpinning the SNRA, and how does the SNRA characterize threats and hazards in terms of "Core Themes?" How does the SNRA relate to the components elements of PPD-8?
- Does the SNRA provide a useful construct in the context of critical infrastructure security and resilience? What are the most important considerations for the critical infrastructure mission area based on the SNRA's core themes?
- What are the major elements of the THIRA process? How does this process

translate to the CISR mission arena?

- What does the THIRA process identify as key sources of threat/hazard information? Are these sources readily accessible to critical infrastructure owners/operators?
- What are the key factors for selecting specific threats and hazards of concern using the THIRA process? What guidance does the THIRA process provide regarding the context associated with threat/hazard identification and assessment?
- How are capability targets identified using the THIRA process? Is a general identification of "capability targets" adequate to drive real risk mitigation in the critical infrastructure world? If not, what would you recommend as a next step in the process?
- Are our critical infrastructures more resilient in a post-Hurricane Katrina and Superstorm Sandy world?
- What are the principal challenges we face in ensuring the security and resilience of our critical infrastructures in light of the complex threat environment in which they operate?

3. **In-Class Exercise:** The instructor will divide the class into two-person teams. Each team will be assigned a specific current/future threat to critical infrastructure to research and discuss as part of today's classroom activities. Topics to be assigned will include the following:
    - Catastrophic Natural Disasters (including High Impact Low Frequency events)
    - Aging Infrastructure
    - Climate Change
    - Space Weather and Geomagnetic Disturbance (GMD)/Electromagnetic Pulse (EMP) Events
    - Terrorists, Active Shooters, and "Insider Threats"
    - Chemical Biological, Radiological, and Nuclear (CBRN) Attacks and Accidental Releases
    - Physical-Cyber Threat Convergence
    - Global Supply Chain Issues
    - Pandemics

Each learner team should be prepared to describe the nature of the particular threat assigned, its relevance and potential impacts to the CISR mission area, and associated risk management approaches in alignment with the THIRA or other risk assessment process. No formal presentation will be required; outside-of-class Internet research is expected.

4. Required Reading:

Brown, Chapter 5.

Collins and Baggett, Chapters 13-15.

U.S. Department of Homeland Security, *Threat and Hazard Identification and Risk Assessment Guide Comprehensive Preparedness Guide (CPG) 201 Second Edition* (2013) http://www.fema.gov/media-library-data/6172ec35e71ec36f662273eb8a0820d8/C

PG_201_THIRA_2nd_Edition_FINAL_20130821.pdf.

U.S. Department of Homeland Security, *Strategic National Risk Assessment* (2011) http://www.fema.gov/media-library-data/20130726-1854-25045-5035/rma_strategic_national_risk_assessment_ppd8_1_.pdf

Strategic National Risk Assessment Executive Summary, 2012, http://www.fema.gov/media-library/assets/documents/29223.

National Information Sharing Consortium, *Essential elements of Information Publication Guidance*, March 2015, http://www.nisconsortium.org/portal/resources/bin/NISC_EEI_Publication_1426695387.pdf

Xavier Guiho, Patrick Lagadec and Erwan Lagadec, *Non-conventional Crises and Critical Infrastructure: Katrina*, 2006, http://www.patricklagadec.net/fr/pdf/EDF-Katrina-Report-31.pdf.

Louise K. Comfort and Thomas W. Haase, *Communication, Coherence and Collective Action: The Impact of Hurricane Katrina on Communications Infrastructure*, 2006, http://www.iisis.pitt.edu/publications/Communication_Coherence_and_Collective_Action-Katrina.pdf.

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

A. Miller and Irving Lachow, National Defense University, *Strategic Fragility: Infrastructure Protection and National Security in the Information Age*, 2008, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA476034&Location=U2&doc=GetTRDoc.pdf.

Congressional Research Service Report, *International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress*, 2010, http://assets.opencrs.com/rpts/R41004_20100318.pdf.

Rand Corporation, *The Lessons of Mumbai*, 2008, http://www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf.

Congressional Research Service, *Banking and Financial Institution Continuity: Pandemic Flu, Terrorism, and Other Challenges*, 2009, http://www.fas.org/sgp/crs/misc/RL31873.pdf.

Atomic Energy Society of Japan, "*Lessons Learned from the Accident at the Fukushima Daiichi Nuclear Power Plant*,"
2011, http://www.aesj.or.jp/en/release/gbcom_kyokun_EN_20110530.pdf.

Foundations of Critical Infrastructure Security and Resilience

Lesson 3: Examining CISR in the Context of the 21ST Century Threat Environment

Lesson 3 Objectives

- Identify and evaluate the various threats and hazards that may impact critical infrastructure within and across the different sectors, and how they can be viewed in an all-hazards risk management approach.
- Explain the major elements of the Strategic National Risk Assessment (SNRA) and the Threat and Hazard Identification and Risk Assessment (THIRA) process, as well as their applicability to the CISR mission area.
- Discuss how the results of the THIRA process can be used to inform investments and capability delivery in the CISR mission area.
- Assess the challenges associated with achieving CISR in the current and projected threat environment.

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 Risk Management Framework

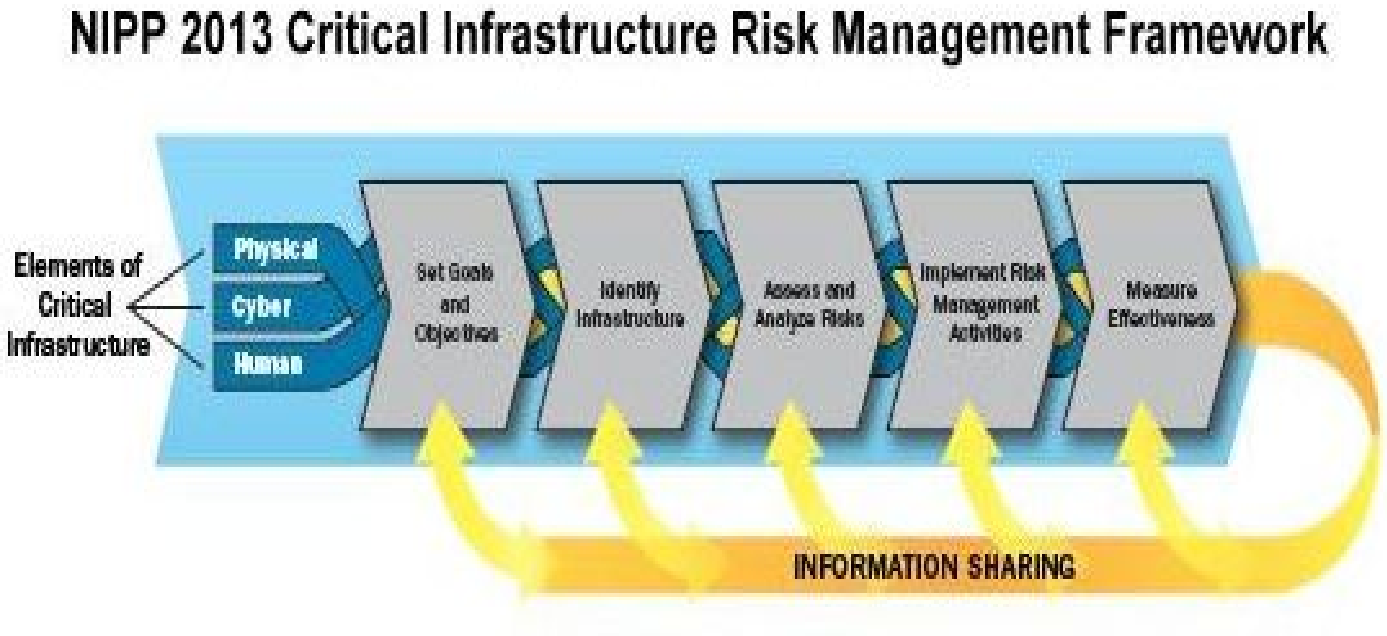


Image: DHS

CI Threat-related Essential Elements of Information (EEIs)

- EEIs are important and standard information items that planners and decision makers need in order to make timely and informed decisions.

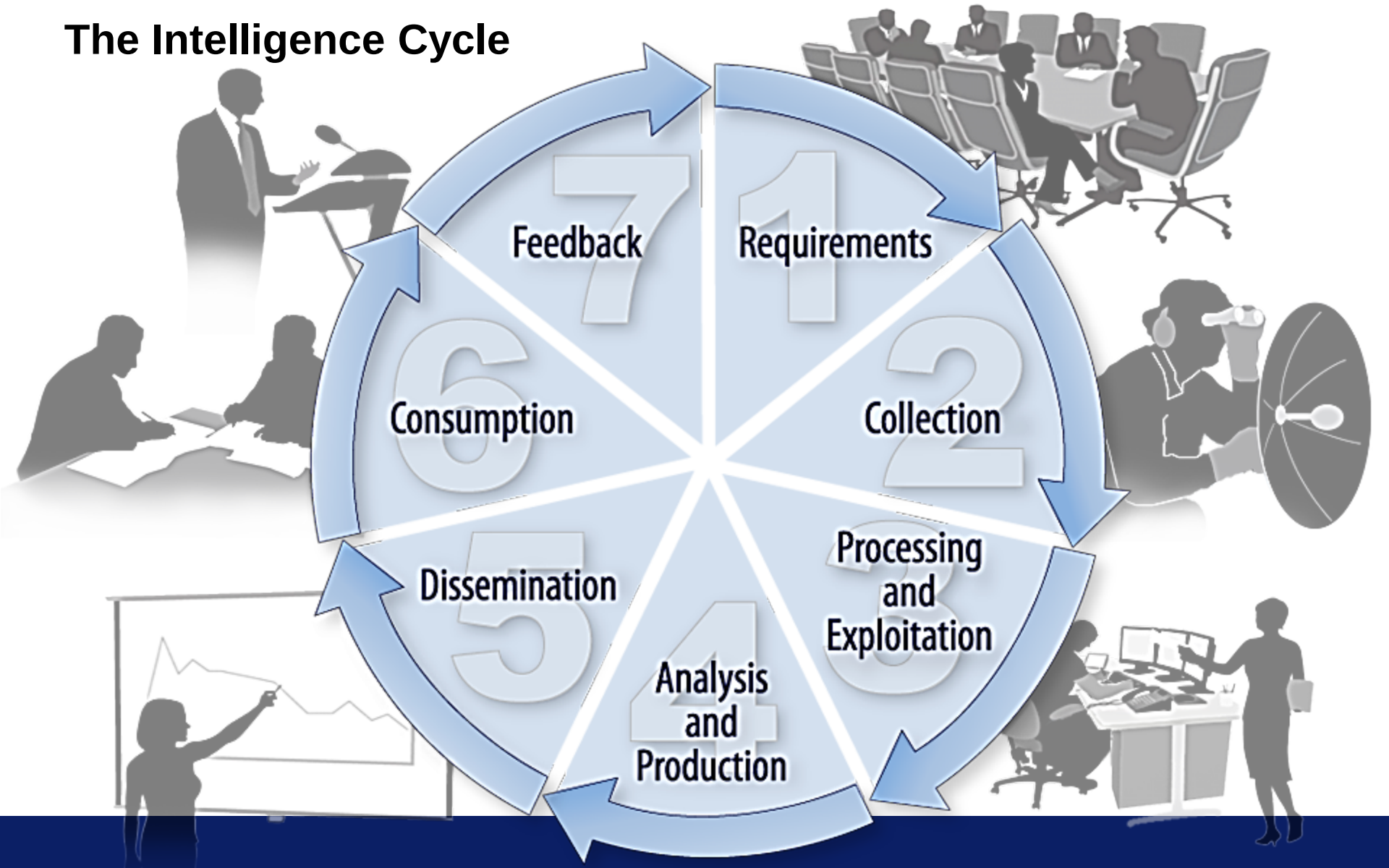
- What are the two primary perspectives of an EEI?
  - Information you need to provide or receive in order to function in your critical role; and
  - Information that needs to be protected from access by a threat actor.

- What would an EEI list look like in the world of CISR (student critical thinking drill)?

CI Threat-related EEIs (Examples)

- Identify and characterize threat or hazard actor/vector
- Identify how the threat/hazard would be recognized or manifest itself
- Identify target/potential communities of impact
- Identify expanse/distribution
- Establish timing parameters/likelihood of recurrence
- Identify vulnerabilities likely to be exploited by threat/hazard
- Identify likely impacts
- Identify potential connections to other threats/hazards

The Intelligence Cycle



Strategic National Risk Assessment

- Identifies risk from known threats and hazards that have the potential to significantly impact the Nation's homeland security (natural hazards, technological/accidental hazards and malicious actor-caused threats/hazards)

- Identifies high risk factors to support development of NPG core capabilities and capability targets

- Supports development of collaborative thinking about strategic needs across prevention, protection, mitigation, response and recovery requirements

- Enables all levels of govn't to share common understanding of Nat'l threats/hazards and resulting risks to enable independent/collaborative risk management

SNRA (Cont.)

- Results are largely classified
- Includes comparison of risks for potential incidents in terms of likelihood (number of events per year) and consequences (loss of life, injuries and illnesses, direct economic costs, social displacement, psychological distress, and environmental impact), as well as an analysis of the uncertainty associated with those incidents
- Historic events provide a useful perspective on homeland security risks; however, changing nature of society and risk landscape means that we must also be prepared for new hazards/threats that result in greater consequences than in the past
- Some events generally cause more localized consequences, while other events, such as human pandemics, may cause consequences that are widely distributed, thus creating different types of impacts for planners to consider

Threat Hazard Identification and Risk Assessment

- The THIRA process:

THIRA (Cont.)

- **Identify Threats/Hazards of Concern.** Based on a combination of experience, forecasting, subject matter expertise and other available resources, identify a list of threats/hazards of primary concern to the community. (Sources?) (Likelihood?) (Severity?) (HILF events?)

- **Give the Threats and Hazards Context.** Describe the threats/hazards of concern, showing how they may affect the community. (time, location, conditions)

- **Establish Capability Targets.** Assess each threat/ hazard in context to develop a specific capability target for each core capability identified in the NPG. (impacts and specific, measurable outcomes; timeframe and LOE)

- **Apply the Results.** For each core capability, estimate resources required to achieve capability targets through the use of community assets and mutual aid, while also considering preparedness activities, including mitigation opportunities.

THIRA (Cont.)

- What's "unique" about THIRA?
  - Broadening the threats and hazards typically considered to include human-caused threats and technological hazards
  - Incorporating the "whole community" into the planning process, including individuals; families; businesses; faith-based and community organizations; nonprofit groups; schools and academia; media outlets; and all levels of government
  - Providing increased flexibility to account for community-specific factors

- Threat/hazard identification based on "likelihood" and "significance"
  - "High Impact, Low Frequency" events???

- Context = time, place, conditions, demographics, built environment characteristics, etc.

THIRA (Cont.)

- THIRA process supports the first two components of the NPS:
  - Identifying and Assessing Risk
  - Estimating Capability Requirements

- THIRA process helps communities answer the following questions:
  - What does the community need to prepare for?
  - What resources are required in order to be prepared?
  - What actions (e.g., mitigation activities) could be employed to lessen or eliminate the threat or hazard?
  - What impacts need to be incorporated into the community's recovery preparedness planning?

- Results of the THIRA process form the foundation for subsequent NPS activities

Lesson 3 In-class Activity

- The class will be divided into two-person teams. Each team will be assigned a specific current/future threat to critical infrastructure to research and discuss as part of today's classroom activities. Topics to be assigned will include the following:
  - Catastrophic Natural Disasters (including High Impact Low Frequency events)
  - Aging Infrastructure
  - Climate Adaptation
  - Space Weather and Geomagnetic Disturbance (GMD)/Electromagnetic Pulse (EMP) Events
  - Terrorists, Active Shooters, and "Insider Threats"
  - Chemical Biological, Radiological, and Nuclear (CBRN) Attacks and Accidental Releases
  - Physical-Cyber Threat Convergence
  - Global Supply Chain Issues
  - Pandemics

- Each learner team will describe the nature of the particular threat assigned, its relevance and potential impacts to the CISR mission area, and associated risk management approaches in alignment with the THIRA or another risk assessment process in use at the sector level.

Discussion Questions

- How does CSIR factor into the overarching PPD-8 construct? How does the NIPP 2013 relate to the PPD-8 construct, particularly regarding the NIPP's approach to risk management?
- Currently, what are the principal threats and hazards to our critical infrastructure assets, systems, and networks? At a sector level?
- How have these threats/hazards evolved over time in terms of potential impacts (magnitude and type)?
- Why would government expand its view of critical infrastructure to encompass targets that have amplifying effects, such as commercial facilities?
- What are the trends regarding international and domestic terrorist acts focused on critical infrastructure assets, systems, and networks?
- What part do our critical infrastructure "target sets" play in the concept of "asymmetric warfare?"

Discussion Questions (Cont.)

- What is the underlying analytical approach underpinning the SNRA, and how does the SNRA characterize threats and hazards in terms of “Core Themes?” How does the SNRA relate to the components elements of PPD-8?

- Does the SNRA provide a useful construct in the context of critical infrastructure security and resilience? What are the most important considerations for the critical infrastructure mission area based on the SNRA’s core themes?

- What are the major elements of the THIRA process? How does this process translate to the CISR mission arena?

- What does the THIRA process identify as key sources of threat/hazard information? Are these sources readily accessible to critical infrastructure owners/operators?

- What are the key factors for selecting specific threats and hazards of concern using the THIRA process? What guidance does the THIRA process provide regarding the context associated with threat/hazard identification and assessment?

Discussion Questions (Cont.)

- How are capability targets identified using the THIRA process? Is a general identification of “capability targets” adequate to drive real risk mitigation in the critical infrastructure world? If not, what would you recommend as a next step in the process?

- What are “Essential Elements of Information” (EEIs) in the context of recognizing and addressing threats to CSIR? How are EEIs formulated, and what role do they play in an emergent threat or incident situation?

- Are our critical infrastructures more resilient in a post-Hurricane Katrina and Superstorm Sandy world?

- What are the principal challenges we face in ensuring the security and resilience of our critical infrastructures in light of the complex threat environment in which they operate?