Lesson 13 Outline

Course Number: XXXX

Course: Foundations of Critical Infrastructure Security and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

LESSON 13 TOPIC: UNDERSTANDING, PLANNING FOR, AND ADDRESSING LONG-TERM AND ENDURING RISKS TO CRITICAL INFRASTRUCTURE AND COURSE WRAP-UP

1. Lesson Goals/Objectives:

- Assess the likely critical infrastructure future operating environment, with a particular focus on dependencies, interdependencies, and technology factors.
- Evaluate long-term and enduring threats to critical infrastructure and corresponding long-term strategies and resources to address them.
- Identify and evaluate various strategic issues that may impact our approach to CISR resilience planning and risk management in the medium (5-10 years) to long term (10-20 years) future.
- Identify and evaluate the types of potential activities and investments required to adequately prepare for the future world of CISR.
- Conduct an overall group "hotwash" of the course and provide individual feedback to help guide future course iterations.

2. Discussion Topics:

- What can we predict about what the critical infrastructure operational environment potentially look like 10-20 years from now? What major changes do you anticipate as we evolve towards this future?
- What will the principal threats and challenges to CISR and cybersecurity be in this future world? Can these be anticipated today? If so, how?
- What insights do we have on the nature of critical infrastructure dependencies and interdependencies in the future? How will technology factor into this assessment?
- What are "convergent technologies" and how are they categorized? How will "convergent technologies" impact the future world of CISR?
- How do we best plan for this future world given the many unknowns and resource constraints that we face today? Will today's priority focus areas set us up for success? Are we focused on the right issues moving forward?
- Is the critical infrastructure partnership organized appropriately to deal with the operational and threat environments of the future? If not, how should the NIPP partnership be strengthened to deal with the operational and threat environments that the future portends?
- How do we set objectives and address planning concerns that transcend the next Federal budget cycle and influence resource decisions across the

partnership?

- How can we achieve truly collaborative and integrated CISR and cybersecurity planning in the future across sectors and jurisdictions?
    - Identification of long-term, enduring threats and hazards
    - Organizing and partnering to address long-term threats and hazards
    - Strategic planning and resource investment
    - Technology Factors

3. In-Class Exercise: Learners will be assigned into teams to develop and informally present and discuss alternative scenarios regarding the future CISR operating and risk environments, as well as related issues and challenges.

4. Required Reading:

http://www.weforum.org/reports/global-risks-report-2015

Mickey McCarter, *Future Homeland Security Threats Comprise Smaller Groups, Cybersecurity Vulnerabilities, Experts Say*, 2012, http://www.hstoday.us/focused-topics/airport-aviation/single-article-page/future-homeland-security-threats-comprise-smaller-groups-cybersecurity-vulnerabilities-experts-say/1477d61bf86af9a2ebb0fcc346a71384.html

Sandra Erwin, Stew Magnuson, Dan Parsons, and Yasmon Tadjdeh, *Top Five Threats to National Security in the Coming Decade*, 2012, http://www.nationaldefensemagazine.org/archive/2012/November/Pages/TopFiveThreatstoNationalSecurityintheComingDecade.aspx

Darrell M. West, *A Vision for Homeland Security in the Year 2025*, 2012, *http://www.insidepolitics.org/brookingsreports/homeland_security.pdf*

The Future of Homeland Security: Evolving and Emerging Threats, 2012, http://www.hsgac.senate.gov/hearings/the-future-of-homeland-security-evolving-and-emerging-threats

Toffler Associates, *Guarding Our Future: Protecting our Nation's Infrastructure*, 2008, http://www.toffler.com/assets/1/6/Guarding-Our-Future.pdf

Toffler Associates, *Five Critical Threats to the Infrastructure of the Future*, 2008, http://www.somanco.com/documents/Five%20Critical%20Infrastructure%20Threats.pdf

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.

Robert McCreight, *Convergent Technologies and Future Strategic Security Threats*,

http://www.au.af.mil/au/ssq/digital/pdf/winter_13/2013winter-McCreight.pdf

Federal Emergency Management Agency, *Critical Infrastructure Long-term Trends and Drivers and Their Implications for Emergency Management*, June 2011, http://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf

Rob Puentes, *Memo to the President: Invest in Infrastructure for Long-term Prosperity*, Brookings Institution, Washington, D.C., 2009, http://www.brookings.edu/research/papers/2009/01/12-prosperity-memo

Foundations of Critical Infrastructure Security and Resilience

Lesson 15: UNDERSTANDING, PLANNING FOR AND ADDRESSING LONG-TERM AND ENDURING RISKS TO CRITICAL INFRASTRUCTURE

Lesson 15 Outcomes/Objectives

- Assess the likely critical infrastructure future operating environment, with a particular focus on dependencies/interdependencies and technology factors.
- Evaluate long-term and enduring threats to critical infrastructure and corresponding long-term strategies and resources to address them.
- Identify and evaluate the strategic choices that may impact our approach to CISR planning in the medium (5-10 years) to long-term (10-20 years) future.
- Identify and evaluate the types of activities and investments that must be undertaken to adequately prepare for the future world of CISR.
- Conduct an overall group “hotwash” and provide individual feedback to help guide future iterations of the course.

10 Global Risks of Highest Concern in 2015

1. Fiscal crises in key economies
2. Structurally high unemployment/underemployment
3. Water crises
4. Severe income disparity
5. Failure of climate change mitigation and adaptation
6. Greater incidence of extreme weather events (floods, storms, fires)
7. Global governance failure
8. Food crises
9. Failure of a major financial mechanism/institution
10. Profound political and social instability

Source: http://www.weforum.org/reports/global-risks-report-2015

2015 Global Risk Report Summary

- Risks considered high impact and high likelihood are mostly environmental and economic in nature: greater incidence of extreme weather events, failure of climate change mitigation and adaptation, water crises, severe income disparity, structurally high unemployment and underemployment and fiscal crises in key economies.

- Risks perceived to be most interconnected with other risks are macroeconomic – fiscal crises, and structural unemployment and underemployment – with strong links between this macroeconomic risk nexus and social issues, such as rising income inequality and political and social instability. The failure of global governance emerges as a central risk that is connected to many different issues.

- 3 things to watch:
  - Instability in an increasingly multipolar world.
  - The “lost generation.”
  - “Digital disintegration.”

Source: http://www.weforum.org/reports/global-risks-report-2015

CISR Mid-term Challenges (5 years Out)

- Increasing frequency of/potential for “mega-disasters”
- Sustainment of public-partnership partnership framework (“waning” of perceived threat, economic crisis, federal/state budgets, competing priorities, bureaucratic politics, etc.)
- Rapid pace of physical-cyber convergence across sectors
- Just-in-time supply chain & global economy
- Emergent asymmetric threats (nation-state & non-state actors: cyber & WMD? ISIS?)
- Strategic fragility of our aging infrastructure base + increasing demand for infrastructure services based on population growth and urbanization
- No common, general international focus on the problem or potential solutions
- Increasing foreign ownership of U.S. critical infrastructure

CISR Long-term Challenges (10-15 Years Out & Beyond)

- Dramatically increased frequency of/potential for “mega-disasters”
- Infrastructure recapitalization (or collapse?)
- Climate change (rise in sea level, ocean acidification, long-duration droughts, etc.)
- “Disruptive” technologies—nanotechnologies, biotechnologies, sensors, transportation automation, ubiquitous data and wireless systems, etc.
- Complete integration of cyber across our CI base
- Hyper-sensitive, just-in-time supply chain considerations
- Hyper-empowered non-state threat actors & other asymmetric threats
- Future water and energy usage
- Population growth, hyper-paced urbanization and coastal migration

Converging Technologies

T

- Technological Convergence: tendency for different systems to eventually evolve, blend, and synergistically reinforce and interact with each other, sharing and extracting resources and energy to produce new and unique metatechnological products and outcomes.

- Examples: *robotics, cybernetics, neuroscience, genomics, artificial intelligence and nanoscience.*

- The Challenge: inadvertent or deliberately engineered combinations, blends and synergistic integration of these technologies which when combined display strategically significant *dual-use* properties.

- Not necessarily subject to U.S. control, protection or governance.

Discussion Questions

- What can we predict about how the homeland security and critical infrastructure risk environments will look in the next decade and beyond?
- What can we predict about what the critical infrastructure operational environment potentially look like 10-20 years from now?
- What will the principal threats and challenges to CISR and cybersecurity be in this future world? Can these be anticipated today? If so, how?
- What insights do we have on the nature of critical infrastructure dependencies and interdependencies in the future? How will technology factor into this assessment?
- What are “convergent technologies” and how are they categorized? How will “convergent technologies” impact the future world of critical infrastructure security and resilience?
- How do we best plan for this future world given the many unknowns and resource constraints that we face today? Will today’s priority focus areas set us up for success? Are we focused on the right issues moving forward?

Discussion Questions

- Is the critical infrastructure partnership organized appropriately to deal with the operational and threat environments of the future? If not, how should the NIPP partnership be organized to deal with the operational and risk environments that the future portends?

- How do we set objectives and address planning concerns that transcend the next Federal budget cycle and influence resource decisions across the partnership?

- How can we achieve truly collaborative and integrated critical infrastructure security and resilience and cybersecurity planning in the future across sectors and jurisdictions?
  - Identification of long-term, enduring threats and hazards
  - Organizing and partnering to address long-term threats and hazards
  - Strategic planning and resource investment
  - Technology Factors

- What tools and data do you suggest government or industry develop or collect to enhance our ability to manage emerging risks?

In-Class Activity

- Learners will organize into their instructor-assigned teams to informally present and discuss alternative scenarios regarding the future CISR operating and risk environments, as well as related issues and challenges.
  - Identification and discussion of long-term, enduring threats and hazards
  - Organizing and partnering to address long-term threats and hazards
  - Strategic planning and resource investment to manage future risk
  - Technology Factors

Course Wrap-up and Critique

- Course Administration
- Structure
- Content
- Method of Delivery
- Classroom Discussions
- In-Class Exercises and Activities
- Research Paper and Oral Presentation
- CISR Incident Management TTX
- Overall Learning Experience