**Course Number: XXXX**

**Critical Infrastructure Security and Resilience: Identifying, Assessing, and Addressing Emergent Threats**

**University of XXXXXX**

**Fall/Spring Semester 20XX**

**name of school:**

**department:**

**professor:**

Telephone Number:

Office Location:

Office Hours:

Email:

Website:

**course description/overview:**

Our critical infrastructure assets, systems, and networks operate within the context of a highly complex and dynamic threat environment. This threat environment is comprised of a diverse and complicated mix of manmade and naturally occurring threats and hazards. From an operating perspective, our critical infrastructure sectors are increasingly interdependent and vulnerable due to the nature of their physical environments, functionality, supply chains, and cyber interconnections. To understand and address existing and emergent threats and enhance both security and resilience in the context of these complexities, government and industry must work together to develop collaborative approaches tailored to the realities of the policy, operational, and threat environments in which our critical infrastructure functions day-to-day.

This course examines the application of an all-hazards threat assessment and risk management framework in the context of critical infrastructure security and resilience. It explores the strategic and operational context provided in the National Infrastructure Protection Plan (NIPP) and discusses the challenges associated with understanding and taking action — including investment strategies— to address a diverse spectrum of threats and hazards across our critical infrastructure sectors and systems. Successful navigation of this extremely complex environment is only possible through collective public-private preparedness, assessment of risk, and planning to enable the effective, efficient management of all-hazards risk. Interestingly, the nature of the threats we face today, and those that will manifest themselves in the future, results in very different approaches and needs relative to the security and resilience of critical infrastructure such as electric power transmission systems, communications systems, healthcare systems, pipelines, transportation grids, etc., and their individual supply chains. This course will provide an in-depth look at the dynamic interplay among these issues.

This course is a 15-lesson graduate-level elective seminar providing a focus on critical infrastructure security and resilience from the perspective of emergent threats. It is designed to promote subject-matter understanding, critical analysis of issues, insight into threat assessment and risk management, and an appreciation of the dynamic and evolving all-hazards threat environment in which our critical infrastructure operates. Specific areas of focus include the examination of a framework for assessing and addressing the critical infrastructure threat environment, as well as the practical application of this framework through a series of case studies of specific types of threats and hazards. The course also features a comprehensive practical examination of critical infrastructure sector stakeholder interaction and key subject-matter areas through in-class discussions, group exercises, and a collaborative written case study project and oral presentation. These “hands-on” applications will reinforce knowledge and critical thinking skills gained throughout the course. In terms of the learner audience, this course assumes a base level of academic knowledge and/or practical experience in the critical infrastructure security and resilience field.

The course begins with a brief review of the current policy and operating environments relative to critical infrastructure security and resilience, including a focus on the various legislative authorities, policy directives, strategies, frameworks, and plans that provide national-level guidance in this subject area. The course then examines the core elements of a framework for identifying, assessing, and addressing emergent threats to critical infrastructure, using the Strategic National Risk Assessment (SNRA) and the Homeland Security Threat and Hazard Identification and Risk Assessment (THIRA) process as benchmarks. This discussion sets the stage for the next section of the course in which learners will examine various specific emergent threats to critical infrastructure including: malicious actors, catastrophic natural disasters, climate change, aging infrastructure, geomagnetic disturbance (GMD)/electromagnetic pulse (EMP) events, pandemics, cyber-physical convergence, and the global nature of critical infrastructure supply chains. This discussion will be further enhanced by student research, a case-study focused collaborative project focused on real world application of the THIRA/SNRA to an infrastructure of concern, and an interactive oral case study presentation.

**credits conferred:** 3

**prerequisites:**

* Masters Degree Course Number XXXX: Introduction to Critical Infrastructure Security and Resilience

**OR**

* Certificate Program Course Number XXXX:Foundations ofCritical Infrastructure Security and Resilience

**course goals/objectives**

This course is designed to enable learners to:

**1. Assess the current policy and operational environments affecting critical infrastructure security and resilience.**

* Course introduction, overview, and learner expectations
* Discussion of framing principles and concepts
* Review of the core elements of the various national policies, strategies, frameworks, plans, and reports that together provide the cornerstone for the U.S. approach to critical infrastructure security and resilience
* Review of the roles and responsibilities of public and private sector critical infrastructure stakeholders

**2. Apply the core elements of a critical infrastructure-focused threat identification, assessment, and risk management framework at national, regional, sector, and system levels.**

* Identifying and assessing threats and hazards: manmade (deliberate & unintentional) and naturally occurring (natural disasters and naturally occurring phenomena)
* Addressing threats (current and future): policies, plans, programs, resource investments, tools and technologies, information sharing, research and development (R&D), etc.
* Adapting and using the Homeland Security THIRA Process and the SNRA to identify, assess, and address all-hazards threats to critical infrastructure

**3. Evaluate various specific critical infrastructure-focused threats and hazards.**

* Catastrophic Natural Disasters (including High Impact Low Frequency events)
* Aging Infrastructure
* Climate Change
* Space Weather and GMD/EMP Events
* Terrorists, Active Shooters, and Other Malicious Actors (both external threat actors and “insider” threat actors)
* Chemical Biological, Radiological, and Nuclear (CBRN) Attacks and Accidental Releases
* Physical-Cyber Threat Convergence
* Global Supply Chain Issues
* Pandemics
* Technical Failures

**4. Evaluate long-term and enduring threats to critical infrastructure and corresponding long-term strategies, capabilities, and resource investments to address them.**

* Identification of long-term, enduring threats and hazards
* Organizing and partnering to address long-term threats and hazards
* Strategic planning, capabilities build-out, and resource investment
* Technology and Research and Development (R&D)

**delivery method/course requirements:**

Course delivery will include mini-lectures, in-class exercises and learner activities, guest speakers, interactive classroom discussions, and a collaborative case study project. The assigned course readings include a variety of resources, such as authoritative readings (legislation, executive orders, policies, plans, and strategies), implementation readings (documents that are responsive to or attempt to fulfill the requirements established by authoritative documents), independent external reviews (U.S. Government Accountability Office (GAO), Congressional Research Service (CRS), etc.), and academic and industry articles and white papers. Learners are expected to familiarize themselves with the assigned topic and associated readings before class and should be prepared to discuss and debate them critically as well as analyze them for biases and from multiple perspectives. The instructor will facilitate discussion through different levels of questioning (factual, analytical, and practical application of the material) to evaluate the depth of the learner’s comprehension of the subject matter addressed.

**grading:**

Classroom Participation and In-Class Exercises 40%

Collaborative Case Study Project 40%

Oral Presentation 20%

Total 100%

**oral/written requirements:**

1. **Collaborative Case Study Project + Oral Presentation (60%):**

Learners will work collaboratively in 2-person teams to develop and present a 20-25 page (double-spaced), written case study of a specific critical infrastructure emergent threat or hazard using the THIRA/SNRA framework examined during the course. The threat presented can be applicable at a national, regional, sector, or infrastructure system level.

The written case study should be organized using the following format: discussion of how the THIRA/SNRA framework will be tailored to meet the requirements of the assignment, discussion of the nature of the threat/hazard forming the focus of the case study, type and extent of infrastructure potentially impacted and associated cascading effects, key stakeholders affected (include key players, authorities, resources, etc.), discussion of potential capabilities/threat mitigation solutions (presentation of alternative solutions/capabilities, identifying pros and cons for each alternative), and final recommendations (policies, strategies, programs, technical solutions, etc.). The recommendations section should clearly describe the rationale for the solution(s)/capability(ies) of choice. The recommendations provided should be supported by authoritative reports, articles, interviews, or other data. Data sources, references, and citations should be included on a separate sheet of paper in the proper format for review.

Each learner team will present the highlights of its case study using the descriptive format provided above to the class during Lessons 13-14. This presentation should involve both team members and be no more than 30 minutes in length.

**The instructor will assign learner team pairings at the end of class on Lesson 3**. The specific case study examined will be at the discretion of each learner team, subject to approval of the instructor. **The completed written project deliverable must be submitted to the instructor via e-mail no later than the beginning of class on Lesson 14 for all project teams.**

1. **Expectations for In-Class Participation (40%):**

Participation includes coming to class prepared, engaging in class discussions, being a full partner in group activities, and dynamic role playing during in-class exercises.

**incorporation of feedback**:

The course instructor will offer multiple opportunities for learners to provide/receive constructive feedback over the period of the course. These feedback channels may take the form of group sessions or individually scheduled sessions with the instructor at any time during the course. Learners also will be afforded the opportunity to complete in-class evaluations at the end of Lesson 6, and at the end of the course. On-line feedback is also encouraged throughout the course. Finally, the instructor will provide written feedback to the learners on the collaborative case study project and team oral presentation. Additional ongoing dialogue with the instructor regarding in-class exercises, case study project development, and oral presentation preparation is highly encouraged.

**course materials:**

There are no textbooks required for this course. All course materials are available online and are identified at the end of each of the individual lesson descriptions that are provided in the Course Outline section that follows. Website information for each reference document is provided in each lesson description.

**additional resources:**

Critical Infrastructure Resource Center: <http://training.fema.gov/EMIWeb/IS/is860a/CIRC/index.htm>

U.S. Department of Homeland Security Office of Infrastructure Protection: <http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm>

U.S. Department of Homeland Security Daily Open Source Infrastructure Report: <http://www.dhs.gov/files/programs/editorial_0542.shtm>

Emergency Management Institute Independent Study Program: <http://training.fema.gov/IS/>

Homeland Security Digital Library:

<http://www.hsdl.org/>

*The International Journal of Critical Infrastructures*: <http://www.inderscience.com/browse/index.php?journalID=58>

*The International Journal**on**Critical Infrastructure Protection* (log-in required)

*The CIP Report*:

<http://cip.gmu.edu/the-cip-report>

*Homeland Security Affairs*:

<http://www.hsaj.org/>

*The Journal of Homeland Security and Emergency Management*: <http://www.bepress.com/jhsem/>

*The Journal of Homeland Security*: <http://www.homelandsecurity.org/journal/Default.aspx>

*The Journal of Homeland Security Education*:

[www.JournalHSE.org](http://www.JournalHSE.org)

*The Journal of Infrastructure Systems* (log-in required)

*The European Journal of Transport and Infrastructure Research*: <http://www.ejtir.tbm.tudelft.nl/index.asp>

*The International Journal of Sustainable Transportation*: <http://www.tandf.co.uk/journals/titles/15568318.asp>

*The Journal of Transportation Law, Logistics & Policy*:

<http://www.atlp.org/journal.html>

*The International Journal of Logistics Management*: <http://www.emeraldinsight.com/products/journals/journals.htm?id=ijlm>

*The International Journal of Electrical Power & Energy Systems*: <http://www.journals.elsevier.com/international-journal-of-electrical-power-and-energy-systems/>

The Global Homeland Security Education Network: <http://www.northumbria.ac.uk/sd/academic/sass/about/socscience/solscres/interdiscnetworks/ghsen/>

**grading scale (school policy dependent): TBD**

**course outline**

**lesson 1 topic: course overview & review of the critical infrastructure security and resilience policy and operating environments**

**1. Lesson Goals/ Objectives:**

* Discuss the scope of the course, administrative requirements, instructional methodology, evaluation criteria, written and oral deliverables, and feedback processes.
* Review the evolution of the critical infrastructure security and resilience policy and operational environments.
* Review the various component elements of the NIPP 2013 (general principles; mission, vision, and goals; stakeholder roles and responsibilities; governance & partnerships; information sharing; risk management; call to action; etc.) and provide examples of how these component elements relate to one another.
* Develop an understanding of how current critical infrastructure security and resilience policies, plans, and partnership set the stage for identifying, assessing, and addressing potential future all-hazards threats.

**2. Discussion Topics:**

* Discuss the current operational environment of the critical infrastructure sectors. How are the sectors evolving in terms of structure and function? How are they alike and how are they different? What are the principal dependencies and interdependencies between sectors? How does this operational environment impact sector preparedness for and the response to and recovery from all-hazards threats?
* Discuss and critique the major tenets of the various policies that are shaping the evolution of this mission area (PPD-21, EO 13636, PPD-8, etc.). What are the major policy drivers of the critical infrastructure security and resilience mission area? How are these various policy drivers interrelated? Are we where we need to be?
* How does policy support strategy and plan development for critical infrastructure security and resilience? Are there significant disconnects? Does current U.S. policy set the stage effectively for critical infrastructure-related preparedness, collaboration, and incident management operations? How does U.S. policy handle the international aspects of critical infrastructure planning and incident management?
* Who is responsible for critical infrastructure security and resilience nationally, regionally, locally, and across the critical infrastructure sectors? What are the principal considerations and concerns in this mission area across sectors and governmental jurisdictions?
* What are the key elements of critical infrastructure security and resilience as discussed in the NIPP 2013? Does this plan provide an approach for addressing stakeholder needs and defining a path forward for stakeholder interaction? Are there major issues included in the NIPP or related to NIPP 2013 implementation that might warrant additional guidance outside the NIPP?
* What are the major “Calls to Action” as presented in the NIPP 2013? How might these calls to action best be considered and implemented?
* What are the key recommendations contained in the 2013 National Infrastructure Advisory Council Report, “Implementing EO 13636 and PPD-21?” Do you concur with these recommendations? Why or why not?
1. **In-Class Exercises:** 1) Learners will be divided into groups to discuss and formulate candidate “national partnership priorities” for critical infrastructure security and resilience as called for in the NIPP 2013. 2) Learners will be divided into groups to discuss how the various “Calls to Action” identified in the NIPP 2013 should further be defined, refined, and implemented through the NIPP public-private partnership.
2. **Required Reading**:

*Presidential Policy Directive-8, National Preparedness* (2011)

<http://www.dhs.gov/presidential-policy-directive-8-national-preparedness>

<http://www.fema.gov/preparedness-1/learn-about-presidential-policy-directive-8#MajorElements> (National Preparedness System)

<http://www.fema.gov/library/viewRecord.do?fromSearch=fromsearch&id=5689>

(National Preparedness Goal)

*Presidential Policy Directive-21, Critical Infrastructure Security and Resilience* (2013)

<http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

*Executive Order 13636, Improving Cybersecurity Critical Infrastructure* (2013)

http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

*NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>.

National Infrastructure Advisory Council, *Implementation of EO 13636 and PPD-21,* November 5, 2013,

<http://www.dhs.gov/sites/default/files/publications/niac-eo-ppd-implementation-report-draft-v10.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>

1. **Additional Recommended Reading:**

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

Congressional Research Service Report*, Critical Infrastructures: Background, Policy, and Implementation*,(June 2010),<http://assets.opencrs.com/rpts/RL30153_20100607.pdf>.

National Infrastructure Advisory Council, *“A Framework for Establishing Critical Infrastructure Resilience Goals,”* (2010), <http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf>

Homeland Security Act, Pub. Law 107-296 (2002),

<http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf>.

**lesson 2 topic: a framework for identifying, assessing, and addressing threats to critical infrastructure (part i)**

**1. Lesson Goals/Objectives**:

* Review the critical infrastructure risk management framework and describe the elements of risk as they relate to critical infrastructure security and resilience.
* Discuss the definitions of “threat” and “hazard.”
* Describe the threat element of risk in the context of critical infrastructure security and resilience and the NIPP 2013.
* Discuss the major deliverables required by PPD-8, including the National Preparedness Goal and Core Capabilities; the National Preparedness System and its National Planning Frameworks and Operational Plans; describe how these various components relate to the Strategic National Risk Assessment (SNRA).
* Discuss the major elements of the Threat and Hazard Identification and Risk Assessment (THIRA) process and its applicability to the critical infrastructure security and resilience mission area and associated capability requirements.

**2. Discussion Topics**:

* How are the terms “threat” and “hazard” defined in the context of critical infrastructure security and resilience?
* How does the NIPP address the issue of identifying and assessing all-hazards threats to critical infrastructure?
* What is the underlying analytical approach underpinning the SNRA, and how does the SNRA characterize threats and hazards in terms of “Core Themes?”
* 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?
* How does the SNRA relate to the core elements of PPD-8? Where/how does planning to address emerging threats to critical infrastructure fit into this picture?
* What are the major elements of the THIRA process? How does this process translate into the critical infrastructure security and resilience mission arena?
* What does the THIRA process identify as key sources of threat/hazard information/data? Are these data 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? If not, what would you recommend as a next step in the process?
* How can the THIRA model be tailored for use in identifying and assessing all-hazards threats to critical infrastructure? In identifying and developing core capabilities and other means to manage risk?
* What does the RAND study, *Emerging Threats and Security Planning,* have to say about identifying and planning for future threats? How does this approach differ from the THIRA model? Does it represent an alternative or a complementary approach to the THIRA model?
* How do efforts to address threats to critical infrastructure contribute to overall national preparedness?
* How does industry identify, understand, and plan to address threats to critical infrastructure? Does industry use the PPD-8 approach?
* Does the private sector have access to the SNRA? How could the THIRA approach be tailored to support private sector threat assessment activities at the owner/operator level?
* How does private sector business continuity planning relate to addressing all-hazards threats?
1. **In-Class Exercise:** Learners will be divided into groups tasked to examine ways in which the THIRA can be adapted for use in the critical infrastructure security and resilience mission area, using sector- and system-level examples.
2. **References:**

SNRA

<http://www.fema.gov/media-library/assets/documents/29223?fromSearch=fromsearch&id=6509>

<http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf>

<http://www.dhs.gov/strategic-national-risk-assessment-snra>

THIRA

<http://www.fema.gov/threat-and-hazard-identification-and-risk-assessment>

<http://www.fema.gov/media-library-data/6172ec35e71ec36f662273eb8a0820d8/CPG_201_THIRA_2nd_Edition_FINAL_20130821.pdf>

<http://training.fema.gov/NTE/_assets/NIC_DRAFT_THIRA_Briefing_20130225.pdf>

**5. Required Reading**:

*NIPP 2013: Partnering for Critical Infrastructure Security and Resilience,* 2013, <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>.

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

George Mason University, The Center for Infrastructure Protection and Homeland Security, *Critical Infrastructure Protection: Elements of Risk*,Various articles, 2007,

<http://cip.gmu.edu/archive/archive/RiskMonograph_1207_rv.pdf>.

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/CPG_201_THIRA_2nd_Edition_FINAL_20130821.pdf> and

<http://www.fema.gov/media-library/assets/documents/27775> and [http://training.fema.gov/NTE/\_assets/NIC\_DRAFT\_THIRA\_Briefing\_20130225.pdf](http://training.fema.gov/NTE/_assets/NIC_DRAFT_THIRA_Briefing_20130225.pdf%22%20%5Ct%20%22_blank)

Brian Jackson and David Frelinger, *Emerging Threats and Security Planning*,2009, <http://www.rand.org/pubs/occasional_papers/2009/RAND_OP256.pdf>.

1. **Additional Recommended Reading:**

<http://www.dhs.gov/presidential-policy-directive-8-national-preparedness>

<http://www.fema.gov/preparedness-1/learn-about-presidential-policy-directive-8#MajorElements> (National Preparedness System)

<http://www.fema.gov/library/viewRecord.do?fromSearch=fromsearch&id=5689>

(National Preparedness Goal)

<http://www.fema.gov/core-capabilities>

**lesson 3 topic: a framework for identifying, assessing, and addressing threats to critical infrastructure (part ii)**

**\*\*special activity: The instructor will make sector assignments and team pairings for the collaborative case study project at the end of class**.

**1. Lesson Goals/Objectives**:

* Articulate the nexus between implementation of the National Preparedness Goal and NIPP 2013, with a focus on core capability development and delivery.
* Describe potential connections between the THIRA process or THIRA-like processes and management of existing and emergent threats.
* Explain how the results of the THIRA process or THIRA-like processes might be used to inform investments in critical infrastructure security and resilience.
* Identify and critique the various approaches to developing and implementing critical infrastructure threat mitigation activities and promoting security/resilience investments within the various critical infrastructure sectors.

**2. Discussion Topics**:

* How does critical infrastructure security and resilience 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?
* How do the Core Capabilities that form part of the National Preparedness System relate to critical infrastructure security and resilience? How does a core capabilities approach tie into the NIPP risk management framework? Is a capabilities-based approach sufficient to address emergent threats to critical infrastructure? Why or why not?
* Identify the general range of risk mitigation strategies and core capabilities relevant to the critical infrastructure security and resilience mission area. What are the criteria for an effective security or resilience investment or capability enhancement?
* Can a THIRA-like process be used to foster and direct investments in preparedness, security, and resilience in the critical infrastructure owner/operator world?
* What are the different approaches to voluntary preparedness and security collaboration and coordination within the various critical infrastructure sectors? How are the issues of threat identification, assessment, and management addressed in each?
* How does government at various levels relate to the private sector in these different sector approaches/models?
* Would a THIRA-like approach at a sector, sub-sector, or facility/system level help to produce a measurable increase in those sectors in which regulations related to critical infrastructure security and resilience are not operative?
1. **In-Class Exercise:** The class will be divided into two-person teams, with each team prepared to discuss the approach used to identify, assess, and address all-hazards threats within a particular critical infrastructure sector or subsector. The teams will also be prepared to discuss how a THIRA-like process might be applied to help inform and promote security and resilience investments within that sector.

**4. Required Reading**:

*NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>.

Department of Homeland Security, *Threat and Hazard Identification and Risk Assessment Comprehensive Preparedness Guide (CPG) 201* *Second Edition,* (2013) <http://www.fema.gov/media-library-data/6172ec35e71ec36f662273eb8a0820d8/CPG_201_THIRA_2nd_Edition_FINAL_20130821.pdf>

“Learn About Presidential Policy Directive-8.” *FEMA* (Last Updated February 11, 2014). <http://www.fema.gov/preparedness-1/learn-about-presidential-policy-directive-8#MajorElements>

“National Preparedness Goal.” *FEMA* (September 1, 2011). <http://www.fema.gov/library/viewRecord.do?fromSearch=fromsearch&id=5689>

“Core Capabilities.” *FEMA* (Last Updated May 6, 2013). <http://www.fema.gov/core-capabilities>

“Mission Areas.” *FEMA* (Last Updated November 28, 2012). <http://www.fema.gov/mission-areas>

Philip Auerswald, Lewis M. Branscomb, Todd M. LaPorte and Erwann Michel-Kerjan, *The Challenge of Protecting Critical Infrastructure,* 2005, <http://opim.wharton.upenn.edu/risk/downloads/05-11-EMK.pdf>.

U.S. Department of Homeland Security, *NIPP Sector-Specific Plans*,

<http://www.dhs.gov/sector-specific-plans> (The lesson prior, the instructor will assign each learner team one of the SSPs to read and understand in detail as part of this lesson’s In-Class Exercise).

**5. Additional Recommended Reading:**

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>.

**lesson 4 topic: threats to critical infrastructure: catastrophic natural disasters**

**1. Lesson Goals/Objectives**:

* Assess the threat to critical infrastructure systems posed by catastrophic natural disasters, the planning context supporting preparation for such disasters, and the potential cascading impacts of such disasters on national security, public health and safety, the economy, and American society.
* Assess the various approaches proposed to address the threat posed by catastrophic natural disasters within and across the critical sectors.
* Identify and evaluate the elements of an effective framework for increasing the resilience of critical infrastructure in the context of catastrophic natural disasters.

**2. Discussion Topics**:

* Characterize the threat posed by catastrophic natural disasters to critical infrastructure systems nationally, regionally, and by sector. How do such disasters potentially impact critical infrastructure operations and services? What are the forecasted trends?
* What were the major cascading impacts to critical infrastructure within and across sectors as a result of Hurricane Katrina, Superstorm Sandy, the Great Eastern Japan Earthquake/ Tsumani/ Fukushima-Daiichi Nuclear Reactor Breach, and other like events? What are the major lessons learned from these events?
* How should such impacts be handled in critical infrastructure risk assessments and planning activities?
* How do the “lifeline functions” identified in NIPP 2013 affect the identification and analysis of cascading impacts likely to result from a catastrophic natural disaster?
* How are threats to infrastructure related to catastrophic natural disasters identified and assessed? How are priorities determined?
* How do the SNRA and the THIRA processes account for the threat posed by catastrophic natural disasters? What is the range of such disasters included in the SNRA and the THIRA process?
* What are the key elements of an effective approach to increase the resilience of the critical sectors in the context of catastrophic natural disasters?
* How does NIPP 2013 address threats to critical infrastructure related to natural disasters? What mechanisms are in place to deal with these types of hazards?
* What specific elements of the NIPP Call to Action would be relevant to enhancing critical infrastructure security and resilience in the context of catastrophic natural disasters?
* How does the National Preparedness Goal capabilities development process apply in the context of catastrophic natural disasters?
* What are the major recommendations of the 2009 National Academy of Sciences, *Sustainable Critical Infrastructure Systems: A Framework for Meeting 21st Century Imperatives*? Do you support the conclusions of this report? Why or why not?
* What are the major recommendations of the 2009 NIAC Report, *Framework for Dealing with Disasters and Related Interdependencies,* and the 2013 Report, *Strengthening Regional Resilience,* in this regard? Do you support the conclusions of these reports? Why or why not?

**3. In-Class Exercise:** Learners will be divided into three groups focused on assessing the impacts to critical infrastructure and lessons learned as a result of Hurricane Katrina, Superstorm Sandy, and the Great Eastern Japan earthquake/tsumani/ Fukushima-Daiichi nuclear reactor breach. Additional Internet research will be needed; no formal presentation will be required.

**4. Required Reading**:

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>.

Congressional Research Service Report*, Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options*, 2006,

<http://assets.opencrs.com/rpts/RL33206_20080912.pdf>.

American Geophysical Union, *Hurricanes and the U.S. Gulf Coast: Science and Sustainable Rebuilding*, June 2006, <http://www.agu.org/report/hurricanes>.

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>.

Jack Spencer, “*U.S. Nuclear Policy after Fukushima: Trust but Modify*,” Backgrounder No. 2557, The Heritage Foundation, 2011, <http://thf_media.s3.amazonaws.com/2011/pdf/bg2557.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>

Gridwise Alliance, *Improving Electric Grid Reliability and Resilience: Lessons Learned from Superstorm Sandy and Other Extreme Events,* June 2013,

<https://www.naseo.org/Data/Sites/1/documents/committees/energysecurity/documents/gridwise-superstorm-sandy-workshop-report.pdf>

National Infrastructure Advisory Council, *Strengthening Regional Resilience*, November 2013,

<http://www.dhs.gov/sites/default/files/publications/Strength-reg-resi-final-report-recomendations.pdf> (Super Storm Sandy lessons learned)

Brandon J. Hardenbrook, *The Need for a Policy Framework to Develop Disaster Resilient*

*Regions*, 2005, [http://www.bepress.com/jhsem/vol2/iss3/2/.](http://www.bepress.com/jhsem/vol2/iss3/2/)

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>.

National Infrastructure Advisory Council, *Framework for Dealing with Disasters and Related Interdependencies*, July 2009, <http://www.dhs.gov/xlibrary/assets/niac/niac_framework_dealingwithdisasters_slides.pdf>

**5. Recommended Additional Reading:**

NIST Technical Note 1476, *Performance of Physical Structures in Hurricane Katrina and Hurricane Rita: A Reconnaissance Report*, (June 2006), <http://www.bfrl.nist.gov/investigations/pubs/NIST_TN_1476.pdf>.

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

T.D. O’Rourke, *Critical Infrastructure, Interdependencies and Resilience*, (2007), [http://www.nae.edu/Publications/Bridge/EngineeringfortheThreatofNaturalDisasters/Criti](http://www.nae.edu/Publications/Bridge/EngineeringfortheThreatofNaturalDisasters/CriticalInfrastructureInterdependenciesandResilience.aspx) [calInfrastructureInterdependenciesandResilience.aspx.](http://www.nae.edu/Publications/Bridge/EngineeringfortheThreatofNaturalDisasters/CriticalInfrastructureInterdependenciesandResilience.aspx)

Tom Ridge and Robert B. Stephan, *Preparing for 21st Century Risks: Revitalizing American Manufacturing to Protect, Respond and Recover*, (July 2012), <http://americanmanufacturing.org/homeland>

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>.

**lesson 5 topic: threats to critical infrastructure: aging and operationally degraded infrastructure systems**

**1. Lesson Goals/Objectives**:

* Assess the threat posed by the aging of our critical infrastructure assets and systems, its planning context, and its potential cascading impacts across national security, public health and safety, the economy, and American society.
* Assess the various approaches proposed to mitigate the threat posed by our aging infrastructure base within and across the critical sectors.
* Identify and evaluate the elements of an effective national strategy for critical infrastructure modernization.

**2. Discussion Topics**:

* Characterize the threat posed by our aging critical infrastructure base nationally, regionally, and by sector.
* What are your thoughts regarding the American Society of Civil Engineers (ASCE) *2013 Report Card for America’s Infrastructure*? The ASCE’s *Failure to Act: The Impact of Current Infrastructure Investment on America’s Economic Future?* What are the sectors and infrastructure systems of most significant concern according to these reports? What are the projected consequences of inaction and maintaining the status quo?
* How are threats related to aging infrastructures identified and assessed? Is there a national gap in this area? How are priorities determined?
* Do the SNRA and the THIRA processes account for the threat posed by aging infrastructures? Explain why or why not.
* What are the various approaches proposed to address the threat posed by our aging infrastructure base within and across the critical sectors? What are their strengths and weaknesses?
* How would the recapitalization of America’s aging infrastructure base be financed? What is the role of government? The role of the private sector?
* How can government at all levels and the private sector work together to address the challenges associated with our aging infrastructure base?
* What are the key elements of an effective national strategy for critical infrastructure modernization? How and by whom should such a strategy be carried out?
* How do you motivate investment in major repairs or replacements versus short-term fixes? How do you incorporate such concerns into complex situations like rate cases for utilities? How do you address differences in projected project costs when one bidder considers aging infrastructure issues and one does not?

**3. In-Class Exercise:** Learners will be divided into two-person groups to discuss the impacts of aging infrastructure on a sector-by-sector basis. The instructor will assign sectors for study at the end of the previous class session. Additional Internet research will be required; no formal presentation is required.

**4. Required Reading**:

American Society of Civil Engineers, *2013 Report Card for America’s Infrastructure*, 2013, <http://www.infrastructurereportcard.org/>

American Society of Civil Engineers, *Failure to Act: The Impact of Current Infrastructure Investment on America’s Economic Future,* 2013,

<http://www.infrastructureusa.org/failure-to-act-%EF%BB%BF%EF%BB%BFthe-impact-of-current-infrastructure-investment-on-americas-economic-future/>

U.S. Department of Homeland Security, *Aging Infrastructure: Issues, Research, and Technology*, 2010,

<http://www.dhs.gov/xlibrary/assets/st-aging-infrastructure-issues-research-technology.pdf>

McDonald, Caroline, *A Bridge Too Far: Repairing America’s Aging Infrastructure*, *Risk* *Management*, February 2014, <http://www.rmmagazine.com/2014/02/01/a-bridge-too-far-repairing-americas-aging-infrastructure/>

Little, Richard G., *Managing the Risk of Aging Infrastructure*, 2012,

<http://www.irgc.org/wp-content/uploads/2012/04/R.-Little_Risk-of-Aging-Infrastructure_revision-Nov2012.pdf>

George Mason University , *The CIP Report*, 12(3), September 2013, <http://cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_September2013_AgingInfrastructure.pdf>

Erickson, Mitchell, D., *A Bridge to Prosperity: Resilient Infrastructure Makes a Resilient Nation,* 2009, <http://view.fdu.edu/files/brkprsericksonapr10.pdf>

U.S. Government Accountability Office, *Physical Infrastructure: Challenges and Investment Options for the Nation's Infrastructure*, GAO-08-763T, 2008, <http://www.gao.gov/products/GAO-08-763T>

U.S. Government Accountability Office, *Approaches and Issues*

*for Financing Drinking Water and Wastewater Infrastructure,* Testimony Before the Subcommittee on Interior, Environment, and Related Agencies, Committee on Appropriations, House of Representatives, March 13, 2008,

<http://www.gao.gov/assets/660/652976.pdf>

Miller, Keith; Costa, Kristina; and Cooper, Donna; *Creating a National Infrastructure Bank and Infrastructure Planning Council,* 2012, [*http://www.americanprogress.org/wp-content/uploads/2012/09/InfrastructureBankReport.pdf*](http://www.americanprogress.org/wp-content/uploads/2012/09/InfrastructureBankReport.pdf)

**5. Recommended Additional Reading**:

Tom Ridge and Robert B. Stephan, *Preparing for 21st Century Risks: Revitalizing American Manufacturing to Protect, Respond and Recover*, July 2012, <http://americanmanufacturing.org/homeland>

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>.

**lesson 6 topic: threats to critical infrastructure: climate change**

**\*\*Special Activity: Learner mid-course written feedback provided to instructor at the end of class.**

**1. Lesson Goals/Objectives**:

* Assess the threat to critical infrastructure systems posed by climate change, its planning context, and its potential cascading impacts across national security, public health and safety, the economy, and American society.
* Assess the various adaptation and mitigation approaches proposed to address the threat posed by climate change within and across the critical sectors.
* Evaluate the elements of the President’s Climate Action Plan.

**2. Discussion Topics**:

* Characterize the threat posed by climate change to critical infrastructure systems nationally, regionally, and by sector. How is climate change impacting critical infrastructure operations and services? What are the forecasted trends?
* How are threats to infrastructure related to climate identified and assessed? Is there a national gap in this area? How are priorities determined?
* What is the National Climate Assessment (NCA)? What does the most recent version of the NCA say about the impacts of climate change regionally and across the critical sectors? What are the principal future trends?
* Do the SNRA and the THIRA processes account for the threat posed by climate change? If not, could they be readily adapted to do so? How?
* How does the National Preparedness Goal capabilities development process apply to the context of global climate change?
* What are the various approaches proposed to address the climate change threat within and across the critical sectors? What are their strengths and weaknesses?
* How do approaches to address threats from climate change differ from approaches to address other more predictable or conventional threats? Can preparedness activities conducted in the context of more predictable natural disasters also apply to climate-related threats?
* How can government at all levels and the private sector work together to heighten awareness and address the challenges associated with climate change?
* What are the key elements of the 2013 *President’s Climate Action Plan*? How does this plan address the threat to critical infrastructure systems and foster critical infrastructure future modernization?
* How will the *President’s Climate Action Plan* affect the operational landscape of the critical sectors, particularly the energy and transportation systems sectors? How are action items in the plan being incentivized? How are other levels of government and the private sector engaged?

**3. In-Class Activity**: Learners will be divided into two-person groups to discuss the impacts of climate change on a sector-by-sector basis, based on information provided in the NCA Report and related source materials. The instructor will assign sectors for study at the end of the previous class session. Additional Internet research will be required; no formal presentation is required.

**4. Required Reading**:

<http://www.globalchange.gov/what-we-do/assessment> (National Climate Change Assessment website)

United States Global Change Research Program, Global Climate Change Impacts in the United States, 2009, <http://library.globalchange.gov/products/assessments/2009-national-climate-assessment/2009-global-climate-change-impacts-in-the-united-states>

Kelly, Cathleen, and Sussman, Fran, *The Crushing Cost of Climate Change: Why We Must Rethink America’s Infrastructure Investments*, February 11, 2014,

http://www.americanprogr, ess.org/issues/green/news/2014/02/11/83936/the-crushing-cost-of-climate-change-why-we-must-rethink-americas-infrastructure-investments/

Neumann, James, *Adaption to Climate Change: Revisiting Infrastructure Norms*, 2009,

<http://www.rff.org/RFF/Documents/RFF-IB-09-15.pdf>

DeConcini, Christina, and Tompkins, C. Forbes, *Impacts of Hurricane Sandy and the Climate Change Connection,* 2012,[*http://www.wri.org/publication/impacts-hurricane-sandy-and-climate-change-connection*](http://www.wri.org/publication/impacts-hurricane-sandy-and-climate-change-connection)

<http://www.epa.gov/climatechange/impacts-adaptation/transportation.html>

(EPA website)

<http://www.ecy.wa.gov/climatechange/2012ccrs/infrastructure.htm>

(Washington State website)

U.S. Government Accountability Office, *Climate Change: Federal Efforts Under Way to Assess Water Infrastructure Vulnerabilities and Address Adaptation Challenges,* 2013, <http://www.gao.gov/products/GAO-14-23>

U.S. Department of Energy, *U.S. Energy Sector Vulnerabilities to Climate Change and Extreme Weather*, 2013 <http://energy.gov/sites/prod/files/2013/07/f2/20130716-Energy%20Sector%20Vulnerabilities%20Report.pdf>

Oak Ridge National Laboratory, *Climate Change and Infrastructure, Urban Systems, and Vulnerabilities*, 2012,

<http://www.esd.ornl.gov/eess/Infrastructure.pdf>

The White House, *The President’s Climate Action Plan*, June 2013

<http://www.whitehouse.gov/sites/default/files/image/president27sclimateactionplan.pdf>

The White House, *President Obama’s Climate Action Plan Progress Report: Cutting Carbon Pollution, Protecting American Communities, and Leading Internationally*, June 2014,

<http://www.whitehouse.gov/sites/default/files/docs/cap_progress_report_update_062514_final.pdf>

**lesson 7 topic: threats to critical infrastructure: space weather and geo-magnetic disturbance/electromagnetic pulse (gmd/emp) events**

**1. Lesson Goals/Objectives**:

* Assess the threat to critical infrastructure systems posed by space weather and GMD/EMP events, the planning context supporting preparation for such events, and the potential cascading impacts of such events across national security, public health and safety, the economy, and American society.
* Assess the various approaches proposed to address the threat posed by space weather and GMD/EMP threats within and across the critical sectors.
* Identify and evaluate the elements of an effective framework for increasing the resilience of critical infrastructure in the context of space weather and GMD/EMP events.

**2. Discussion Topics**:

* Characterize the threat posed by space weather and GMD/EMP events to critical infrastructure systems nationally, regionally, and by sector. How do such events potentially impact critical infrastructure operations and services, particularly within the electricity sector? Impacts on other sectors based on linkages to and dependencies on the electricity sector?
* What does DHS say about the potential impacts of GMD/EMP events on industrial control systems within the critical infrastructure sectors?
* With what frequency is it anticipated that such events, on a catastrophic scale, are likely to occur? Can space weather events be predicted?
* What were the impacts of the 1989 GMD/EMP event on Hydro Quebec? What were the principal lessons learned from this experience that might have value in preparing for future events of equal or greater intensity?
* How are threats to infrastructure related to space weather and GMD/EMP events identified and assessed? How are priorities determined?
* How do the SNRA and the THIRA processes account for the threat posed by space weather and GMD/EMP events? What is the range of such events included in the SNRA and the THIRA process?
* How does the National Preparedness Goal capabilities development process apply to the context of space weather and EMP threats?
* Can preparedness activities conducted in the context of more likely catastrophic natural disasters also have applicability to catastrophic space weather and GMD/EMP events?
* What are the key elements of an effective approach to increase the resilience of the critical sectors in the context of space weather and GMD/EMP events?
* What are the principal recommendations of the 2009 Department of Energy/North American Electric Reliability Corporation (NERC) High Impact Low Frequency (HILF) Event Report and the 2012 DOE Report, *Effects of Geomagnetic Disturbances on the Bulk Power System,* regarding GMD/EMP threats?
* Does the January 2014 report issued by the State of Maine Public Utilities Commission reach similar conclusions? How does the state perspective differ from the national/federal perspective on this issue?
* What are the ways in which awareness can be heightened and a proactive preparedness posture for HILF events, such as GMD/EMP events, be incentivized?
* Is there a clear “business case” established that serves to spur investments in preparedness for GMD/EMP events?

**3. Required Reading**:

U.S. Department of Homeland Security, ICS-CERT, *Advisory (ICSA-11-084-01), Solar Magnetic Storm Impact on Control Systems* March 2011*,*

<https://ics-cert.us-cert.gov/advisories/ICSA-11-084-01>

North American Electricity Reliability Corporation, *High-Impact Low-Frequency Event Risk to the North American Bulk Power System*, 2010, <http://www.nerc.com/files/HILF.pdf>

<http://www.pjm.com/~/media/committees-groups/committees/oc/20120313/20120313-item-12-geomagnetic-disturbances-report.ashx> (HILF Report Briefing)

<https://www.ferc.gov/whats-new/comm-meet/2012/101812/E-2.pdf> (Notice of Proposed Rule Making)

[https://www.frcc.com/Standards/RSProjectsUpdateReports/NERC%20FRCC%20Standards%20Under%20Development%20Reports%20(pdf)%202013/NERC%20FRCC%20Reliability%20Standards%20Project%20Updates%2009.25.2013.pdf](https://www.frcc.com/Standards/RSProjectsUpdateReports/NERC%20FRCC%20Standards%20Under%20Development%20Reports%20%28pdf%29%202013/NERC%20FRCC%20Reliability%20Standards%20Project%20Updates%2009.25.2013.pdf) (HILF Event Standards Highlights)

U.S. Department of Energy, *Effects of Geomagnetic Disturbances on the Bulk Power System*, 2012,

<http://www.balch.com/files/upload/2012NERCGMDReport.pdf>

Maine Public Utilities Commission, *Report to the Legislature Pursuant to Resolves 2013, Chapter 45, Regarding Geomagnetic Disturbances (GMD) and Electromagnetic Pulse (EMP),* January 2014,

<http://www.scribd.com/doc/201668925/Maine-Public-Utilities-Commission-Report-on-GMD-EMP-Threat>

<http://www.naruc.org/Filings/12%202812%20NARUC%20GMD%20Comments%20RM12-22-000%20w%20certificate.pdf> (National Association of Regulated Utilities Commissioners Filing)

**4. Additional Recommended Reading:**

<http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf>

(EMP Commission Report)

**lesson 8 topic: threats to critical infrastructure: terrorists, active Shooters, and other malicious actors**

**1. Lesson Goals/Objectives**:

* Assess the nature of the threat to critical infrastructure systems posed by a diverse set of malicious actors, the planning context supporting preparation for malicious actor events, and the potential impacts of such events.
* Assess the various approaches proposed to address the malicious actor threat within and across the critical sectors.
* Identify and evaluate the elements of an effective framework for enhancing the security and resilience of critical infrastructure in the context of malicious actor threats.

**2. Discussion Topics**:

* Characterize the threat posed by terrorists, active shooters, and other malicious actors to critical infrastructure assets and systems nationally, regionally, and by sector. What are the typical motivations of the various malicious actors that have the potential to disrupt our critical infrastructures and harm our critical work force?
* How do such threats potentially impact critical infrastructure operations and services? What are the likely cascading impacts? What are the forecasted trends?
* What were the major impacts to critical infrastructure as a result of malicious actor events at home and abroad over the past decade, including the Madrid and London mass transit events, Boston Marathon bombings, Volgograd train terminal attack, attacks on electric grid nodes, various school and commercial facilities/shopping mall shootings, and other like events?
* How are malicious actor threats to infrastructure identified and assessed? How are priorities determined?
* How do the SNRA and the THIRA processes account for the threat posed by malicious actors? What is the range of malicious actor events included in the SNRA and the THIRA process? Which types of events are most likely? Which are the most consequential?
* How does the National Preparedness Goal capabilities development process apply to the context of malicious actor threats?
* What are the key elements of an effective approach to increase the security of the critical sectors in the context of malicious actor threats? How do these approaches vary by malicious actor type?
* What role does resilience play in mitigating threats from a malicious actor incident?
* What are the major lessons learned from previous malicious actor attacks on critical infrastructure assets and systems, work place environments, and public assembly areas? How have these lessons learned informed future preparedness investments and initiatives and/or government action in the sectors of concern?
* How does the 2008 NIAC Report, *The Insider Threat to Critical Infrastructure*, characterize this type of threat? How significant is this threat across the critical sectors? What are the major obstacles that complicate the addressing of the insider threat? What are the primary recommendations provided to overcome these obstacles?

**3. In-class activity:** The class will be organized into two-person teams, with each team responsible for discussing a case study focusing on a past malicious actor attack on critical infrastructure assets or systems in the U.S. or abroad. The discussion should include a description of the attack, including tactics, techniques, and procedures used; primary and secondary consequences of the attack; and lessons learned from the event that contribute to more effect prevention, protection, and/or response. The instructor will make case study assignments the lesson prior; additional Internet research will be required.

1. **Required Reading**:

Congressional Research Service Report, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*,2010,

<http://www.fas.org/sgp/crs/terror/R41070.pdf>.

Bill Johnstone, *New Strategies to Protect America: Terrorism and Mass Transit after London and Madrid*, 2007, <http://www.americanprogress.org/issues/security/news/2005/08/10/1592/new-strategies-to-protect-america-terrorism-and-mass-transit-after-london-and-madrid/>.

The 2012 Critical Infrastructure Symposium: *Lessons Learned from Past Attacks on America’s Infrastructure*,Raymond H. Bennett, Ph.D., P.E., Baker Engineering and Risk Consultants Inc., 2011,

<http://tisp.org/index.cfm?pid=12831>

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

Congressional Research Service Report, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*,2010,

<http://www.fas.org/sgp/crs/terror/R41070.pdf>.

Mark Holt and Anthony Andrews, *Nuclear Power Plants: Vulnerability to Terrorist Attack*,2007, <http://www.fas.org/sgp/crs/terror/RS21131.pdf>.

Federal Emergency Management Agency, *Boston Marathon Bombings: The Positive Effect of Planning and Preparation on Response,* 2013

<https://www.llis.dhs.gov/sites/default/files/Boston%20Marathon%20Bombings%20Positive%20Effects%20of%20Preparedness_0.pdf>

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 11(9), March 2013, <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/March2013_ActiveShooter.pdf>

U.S. Senate, Committee on Homeland Security and Governmental Affairs, *Lessons Learned from the Boston Marathon Bombings: Preparing for and Responding to the Attack,* July 2013,[*https://www.hsdl.org/?view&did=740471*](https://www.hsdl.org/?view&did=740471)

<http://www.nationalterroralert.com/2013/01/20/dhs-launches-new-active-shooter-preparedness-webpage/>

(Links to Various DHS active shooter planning guidelines, programs and tools)

National Infrastructure Advisory Council, *The Insider Threat to Critical Infrastructures*, 2008,

<http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf>

Brian Jackson and David Frelinger, *Emerging Threats and Security Planning*,2009, <http://www.rand.org/pubs/occasional_papers/2009/RAND_OP256.pdf>.

U.S. Government Accountability Office, *Freight Rail Security: Actions have been Taken to Enhance Security, but the Federal Strategy can be Strengthened and Security Efforts Made Better*, 2009, <http://www.gao.gov/new.items/d09243.pdf>.

1. **Additional Recommended Reading:**

<http://www.training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-906>

(Security in the Workplace Training)

<http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-907>

(Active Shooter Training)

U.S. Department of Homeland Security, *Active Shooter: How to Respond*, 2008,

<http://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf>

<https://www.southerngas.org/sga-blog/2013/11/15/fema-online-course-protecting-critical-infrastructure-against-insider-threats/>

(Insider Threat Training)

The 9/11 Commission Report, *Final Report of the National Commission on Terrorist Attacks Upon the United States*, 2004,

<http://www.9-11commission.gov/>. (Chapters 2, 3, 6 and 7 only)

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

**lesson 9 topic: threats to critical infrastructure: cbrn-based weapons of mass destruction (wmd) and accidental releases/contamination**

**1. Lesson Goals/Objectives**:

* Assess the threat to critical infrastructure systems posed by Chemical, Biological, Radiological, Nuclear (CBRN) threats, whether deliberate attacks or accidental releases/contamination, the planning context supporting preparation for such events, and the potential cascading impacts of such events across national security, public health and safety, the economy, and American society.
* Assess various approaches proposed to address the threat posed by CBRN events within and across the critical sectors.
* Identify and evaluate the elements of an effective framework for increasing the resilience of critical infrastructure in the context of CBRN events.

**2. Discussion Topics**:

* Discuss the various types of potential CBRN events, both manmade and accidental in nature.
* Characterize the threat posed by CBRN events to critical infrastructure systems nationally, regionally, and by sector. How do such events potentially impact critical infrastructure operations and services? What were the major critical infrastructure impacts related to the Fukushima-Daiichi nuclear disaster and the Deepwater Horizon oil spill?
* What are the capabilities of our various potential adversaries (nation states and non-state actors) in the CBRN arena? How would a CBRN-based attack on critical infrastructure differ from a more conventional attack vector? How would a CBRN attack or accidental release complicate critical infrastructure response and restoration activities?
* How are threats to infrastructure related to CBRN events identified and assessed? How are priorities determined?
* How do the SNRA and the THIRA processes account for the threat posed by CBRN events? What is the range of such events included in the SNRA and the THIRA process?
* What are the major findings and recommendations of the 2008 Report, *Report of the Commission on the Prevention of WMD Proliferation and Terrorism?* How do these findings/recommendations relate to the critical infrastructure security and resilience mission area?
* What do the 2011 and 2012 GAO reports referenced below have to say about DHS’ use of CBRN risk assessments to inform plan and resource investments? What are the major findings and recommendations of these reports? How would adoption of the GAO recommendations be of value in the critical infrastructure security and resilience mission area?
* How does the National Preparedness Goal capabilities development process apply to the context of CBRN events and related impacts to critical infrastructure?
* What are the key elements of an effective approach to increase the security and resilience of the critical sectors in the context of catastrophic CBRN events?
* What were the major factors impacting critical infrastructure restoration and recovery in the aftermath of the Fukushima-Daiichi nuclear disaster and the Deepwater Horizon oil spill? What were the major lessons learned from the response to these events across the PPD-8 mission area frameworks?
* How can government at all levels and the private sector work together to address CBRN-related concerns?
* Can capabilities designed for use in the context of accidental CBRN events be repurposed to address malicious actor threats? Would there be any significant gaps in using this approach?
* Can potential malicious actor attacks against our food, agriculture, and water sectors be considered as a CBRN threat? Why or why not?
* How are threats to our food, agricultural, and water sectors identified and assessed? What are the principal threats in these areas?
* How do the food, agriculture, and water sectors address terrorist and other malicious actor threats? Accidental contamination?

**3. In-Class Activity**: For this lesson, the class will be broken down into three teams representing chemical, radiological, and biological threats/hazards. Each team will be prepared to discuss its assigned threat, including the nature of the threat, potential consequences associated with an attack or accident related to the assigned threat, and best practices for addressing the threat across the prevention, protection, and response mission areas. Additional Internet research will be required in order to incorporate real world examples into the discussion; no formal presentation is required.

**4. Required Reading**:

<http://www.ceep.ca/education/CBRNintrosheet.pdf> (CBRN definitions and characterization by event type)

Congressional Research Service, *“Dirty Bombs”: Technical Background, Attack Prevention and Response, Issues for Congress,* 2011, <https://www.fas.org/sgp/crs/nuke/R41890.pdf>

*World at Risk: Report of the Commission on the Prevention of WMD Proliferation and Terrorism, 2008,*

<http://www.cfr.org/terrorism/world-risk-report-commission-prevention-wmd-proliferation-terrorism/p17910>

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, *National Preparedness: DHS and HHS Can Further Strengthen Coordination for Chemical, Biological, Radiological, and Nuclear Risk Assessments,* 2011, <http://www.gao.gov/products/GAO-11-606>

Austen Givens, *Deepwater Horizon Oil Spill Is an Ominous Sign for Critical Infrastructure's Future,* May 27, 2011, http://www.emergencymgmt.com/disaster/Deepwater-Horizon-Oil-Spill-Critical-Infrastructure-052711.html

Okada Norio, Tao Ye, Yoshio Kajitani, Peijun Shi, and Hirokazu Tatano, *The 2011 Eastern Japan Great Earthquake Disaster: Overview and Comments,* 2011,

<http://download.springer.com/static/pdf/779/art%253A10.1007%252Fs13753-011-0004-9.pdf?auth66=1400590230_13d917da8b0eca8255c3aede3dc28770&ext=.pdf>

Charles Perrow, *Fukushima and the inevitability of accidents, Bulletin of the Atomic Scientist,* 2011 <http://scholar.google.com/scholar?start=10&q=fukushima+disaster+critical+infrastructure+impacts&hl=en&as_sdt=0,47&as_vis=1>

James Carafano, *The Great Eastern Japan Earthquake: Assessing Disaster Response and Lessons for the U.S., May 2011,* <http://www.heritage.org/research/reports/2011/05/the-great-eastern-japan-earthquake-assessing-disaster-response-and-lessons-for-the-us>

Bipartisan WMD Terrorism Research Center, *Bio-Response Report Card*, 2011,

<http://www.wmdcenter.org/wp-content/uploads/2011/10/bio-response-report-card-2011.pdf>

U.S. Government Accountability Office, *Homeland Security: Challenges for the Food and*

*Agriculture Sector in Responding to Potential Terrorist Attacks and Natural Disasters*, September 2011,

<http://www.gao.gov/assets/130/126937.pdf>

U.S. Government Accountability Office, *Homeland Security: Actions Needed to Improve Response to Potential Terrorist Attacks and Natural Disasters Affecting Food and Agriculture*, August 2011, <http://www.gao.gov/products/GAO-11-652>

Claudia Copeland, *Terrorism and Security Issues Facing the Water Sector*, 2009, <http://www.fas.org/sgp/crs/terror/RL32189.pdf>.

**5. Additional Recommended Reading:**

Philip Auerswald, Lewis M. Branscomb, Todd LaPorte, and Erwann Michel-Kerjan,

*The Challenge of Protecting Critical Infrastructure*,2005, <http://opim.wharton.upenn.edu/risk/downloads/05-11-EMK.pdf>.

**lesson 10 topic: threats to critical infrastructure: physical-cyber convergence**

**1. Lesson Goals/Objectives**:

* Discuss the multi-dimensional, evolving nature of the cyber threats and challenges that impact the critical infrastructure security and resilience mission area.
* Explain how the various types of cyber threats to critical infrastructure systems are identified and assessed.
* Assess the different sector perspectives on cybersecurity as well as the various approaches used to address cyber threats and secure the cyber components of critical infrastructure systems.
* Identify and evaluate the elements of an effective cyber security risk management framework.

**2. Discussion Topics**:

* How do we define the term “threat” as it relates to the cyber domain? What are some examples?
* What are the principal threats and challenges associated with the cyber domain as they pertain to critical infrastructure security and resilience?
* Who “owns” the cyber problem? On the government side? On the private sector side? How does each party communicate and coordinate with the other to jointly address cyber threats?
* How do Supervisory Control and Data Acquisition (SCADA) system concerns relate to the critical infrastructure sectors? What is the nature of the cyber threat in relation to SCADA vulnerabilities?
* How are the various critical infrastructure sectors dealing with the evolving threat to SCADA systems?
* How are cyber threats assessed and mitigated? How can the THIRA process be used to help identify, assess, and understand cyber threats?
* What are the major elements of the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity?* Does this framework offer a useful approach in enabling the identification, assessment, and management of cyber threats? Why or why not.
* How do we know when we are making a difference in managing threats in this domain? How do we avoid “shifting risk” in this arena and address the threat in a definitive way?
* How does the National Preparedness Goal capabilities development process relate to understanding and mitigating cyber threats?
* What are the core elements of an effective cybersecurity strategy? How does the concept of “defense in depth” apply to the world of cybersecurity?
* Discuss the major components of the USCERT *Cross Sector Roadmap for Cyber-Security of Control Systems.* Does the approach outlined therein lay out a viable path forward in addressing cyber threats to SCADA systems? Why or why not?
* Discuss the major components of the U.S.’s *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.* What are the strengths and weaknesses of the U.S. approach?

**3. In-Class Activity**: For this lesson, the class will be broken down into two teams. Each team will discuss and catalog the “pros and cons” of the *Framework for Improving Critical Infrastructure Cybersecurity* issued by the NIST, with an eye toward its applicability to the identification, assessment, and management of cyber threats within and across the critical infrastructure sectors.

**4. Required Reading**:

Industrial Control Systems-Cyber Emergency response Team (ICS-CERT), *Cyber Threat Source Descriptions*, <https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions>

Georgia Tech Information Security Center, Security Summit 2011, *Emerging Cyber Threats Report,* *2012*, <http://www.gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf>.

National Infrastructure Advisory Council, *Convergence of Physical and Cyber Technologies and Related Security Management Challenges*, 2007,

<http://www.dhs.gov/xlibrary/assets/niac/niac_physicalcyberreport-011607.pdf>

North American Electricity Reliability Corporation, *High-Impact Low-Frequency Event Risk to the North American Bulk Power System*, 2010, <http://www.nerc.com/files/HILF.pdf> (Physical-Cyber Threat Section)

U.S. Government Accountability Office, *Cyber Security: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats*,2010,

<http://www.gao.gov/new.items/d10834t.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 7(8), February 2009, <http://cip.gmu.edu/archive/CIPHS_TheCIPReport_February2009_SCADA.pdf>.

The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

Mariana Hentea, *Improving Security for SCADA Control Systems*, 2008,

<http://ijikm.org/Volume3/IJIKMv3p073-086Hentea361.pdf>.

US-CERT, *Cross-Sector Roadmap for Cybersecurity of Control Systems*, September 2011, <https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/Cross-Sector_Roadmap_9-30.pdf>

National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity V*ersion 1.0, February 2014, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>

**5. Additional Recommended Reading:**

U.S. Department of Homeland Security, Control Systems Security Program, [http://www.us-cert.gov/control\_systems/index.html.](http://www.us-cert.gov/control_systems/index.html)

U.S. Department of Homeland Security, Recommended Practices for ICS Security, <http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html>.

The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009,

<http://whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

The Comprehensive National Cybersecurity Initiative, 2010, [http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.](http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative)

Executive Order 13636, Improving Critical Infrastructure Cybersecurity, 2013, <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

**lesson 11 topic: threats to critical infrastructure: supply chain security**

**1. Lesson Goals/Objectives**:

* Explain how supply chain security issues impact critical infrastructure operations and functionality within and across sectors.
* Assess how supply chain-related issues affect incident response decision making and infrastructure restoration operations.
* Analyze supply chain issues in terms of the critical infrastructure threat assessment and mitigation processes.
* Identify and evaluate the elements of a successful global supply chain strategy.

**2. Discussion Topics**:

* What is meant by “Supply Chain Security” in the context of the critical infrastructure security and resilience mission area?
* Do supply chain security issues represent an all-hazards threat to critical infrastructure systems? How do supply chain issues relate to critical infrastructure risk?
* How do supply chain issues manifest themselves in specific sectors? What risk management strategies do individual sectors use to address supply chain risks?
* How are infrastructure dependencies/interdependencies typically considered by governments and corporations in the threat assessment process? How do supply chain security issues complicate traditional approaches to risk assessment and management?
* Can the THIRA process be tailored to apply to the consideration of supply chain security as a threat to critical infrastructure operations?
* How does the National Preparedness Goal capabilities development process apply to the supply chain security issue area?
* How can supply chain issues best be accounted for in the planning process within and across the critical sectors and international borders?
* What are the major elements of a successful supply chain security strategy? How do these elements relate to one another?
* What are the major obstacles/impediments to global supply chain security?
* What are the major goals and guiding principles that underpin the U.S. National Strategy for Global Supply Chain Security? How does the Strategy propose to reduce offshore threats beyond the control of the U.S.?
* How can a global supply chain security strategy best be implemented, and is there an appropriate mechanism(s) through which implementation could be accomplished and/or incentivized?
* How do we achieve domestic critical infrastructure security and resilience and cybersecurity in the context of a global economy?

**3. In-Class Activity**: Learners will be divided into two-person teams and will be prepared to discuss critical infrastructure supply chain security issues in the context of a real world incident of their choice such as the Japanese Tsunami, Iceland Volcano, Northeast Power Blackout, etc.). The focus of the discussion will be on assessment of the potential threat, impacts to infrastructure systems, response and infrastructure restoration issues, and lessons learned for future threat mitigation. Learners will also be prepared to discuss how the PPD-8 capabilities development process could be used to enable mitigation of supply chain security issues in the context of like threats/hazards in the future. This assignment will require additional Internet research. No formal presentation will be required.

**4. Required Reading**:

The White House, *National Strategy for Global Supply Chain Security*, January 2012, <http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf>

T.D. O’Rourke, *Critical Infrastructures, Interdependencies, and Resilience*, Spring 2007, <http://www.nae.edu/Publications/Bridge/EngineeringfortheThreatofNaturalDisasters/CriticalInfrastructureInterdependenciesandResilience.aspx>

National Defense University, *Strategic Fragility: Infrastructure Protection and National Security in the Information Age*, 2008, <http://www.carlisle.army.mil/DIME/documents/Miller%20and%20Lachow%20Strategic%20Fragility.pdf>.

The Infrastructure Security Partnership, *The Infrastructure Security Partnership, Infrastructure Resilience, and Interdependencies*, March 2010, <http://www.tisp.org/index.cfm?cdid=11972&pid=10261>.

Dave Thomas, Trey Hanbury, Ray Rutngamlug, and A.J. Burton. *Super Storm Sandy Foreshadows a New Paradigm of Protecting Critical Communications and Electric Infrastructure*, 2012,

<http://www.hlregulation.com/2012/11/12/superstorm-sandy-foreshadows-a-new-paradigm-for-protecting-critical-communications-and-electric-infrastructure/>

George Mason University, The Center for Infrastructure Protection and Homeland Security (CIP/HS), *The CIP Report*, 10(1), July 2011,

<http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_July2011_GlobalSupplyChain.pdf>.

International Atomic Energy Agency, *Report of Japanese Government to IAEA Ministerial Conference on Nuclear Safety-Accident at TEPCO’d Fukushima Nuclear Power Stations*,June 7, 2011, <http://www.iaea.org/newscenter/focus/fukushima/japan-report/>.

**5. Additional Recommended Reading:**

Tom Ridge and Robert B. Stephan, *Preparing for 21st Century Risks: Revitalizing American Manufacturing to Protect, Respond and Recover*, July 2012, <http://americanmanufacturing.org/homeland>

**lesson 12 topic: threats to critical infrastructure: global pandemics**

**1. Lesson Goals/Objectives**:

* Assess the nature of the global pandemic threat, its planning context, and its potential impact on critical infrastructure sectors and systems.
* Assess the various approaches used to address the pandemic threat within and across the critical infrastructure sectors.
* Identify and evaluate the elements of an effective global pandemic risk management framework.

**2. Discussion Topics**:

* What is a “global pandemic” and how does it spread? What are the options for reducing transmissibility and containing its spread?
* What are the various national alert stages governing the response to a pandemic outbreak?
* What is the relevance of a global pandemic to critical infrastructure sectors and systems? What are the likely impacts of a global pandemic nationally, regionally, and within the critical sectors, particularly regarding the critical infrastructure work force?
* What are the roles and responsibilities of the various levels of government and the private sector in preparing for, responding to, and recovering from the pandemic threat? Who is responsible for assessing the extent of the threat, communicating this information to the critical sectors, and how does this process work?
* How does the risk management framework described in the NIPP account for/apply to pandemic threats?
* How does the National Preparedness Goal development process help to address the pandemic threat to the critical infrastructure work force?
* How do government and private sector entities plan against the pandemic threat? Is there an informed, collaborative effort between government and industry in the context of this threat?
* What are the major planning assumptions underpinning an effective pandemic risk management strategy?
* What are the various approaches to addressing the outbreak and spread of a global pandemic? What implications will these various approaches have within and across critical infrastructure sectors?
* How should planners consider potentially significant economic side effects and social consequences that, when coupled with the health impact assumptions, may substantially compound the direct effects on critical infrastructure owners/operators and the work force?
* How do planners assess the specific implications for each business’ operations from the direct health impacts combined with the proposed disease containment strategies and incorporate these considerations into the business’ pandemic plan?
* What are the major elements of the DHS Continuity of Operations-Essential (COP-E) Planning Guide for pandemic influenza? Does this guide provide sufficient information to allow business contingency planners to address key actions needed to identify essential functions, people, and material within/across sectors? What alternative methods does it propose to protect and sustain essential functions, people, and material at each phase of a pandemic, from preparation through recovery?
* What role does effective public-private sector strategic communication play in addressing the pandemic threat?

**3. In-Class Exercise**: Learners will be organized into three teams. Each team will be assigned to discuss one of the three specific phases of the pandemic threat: preparedness, response, and recovery. The discussions should include a characterization of the pandemic threat itself during that phase, impacts on critical infrastructure operations and the work force, and approaches to mitigate the threat corresponding to that phase. Sector-specific case studies should be used whenever possible to highlight key points. Activity may require additional Internet research. No formal presentation will be required.

**4. Required Reading**:

CDC, *Business/Employers Influenza Toolkit*, <http://www2c.cdc.gov/podcasts/player.asp?f=4165517> (podcast)

“About Pandemics,” *Flu.gov*, <http://www.flu.gov/pandemic/about/index.html>

“Business Pandemic Influenza Planning Checklist,” *Flu.gov*, <http://www.flu.gov/planning-preparedness/business/businesschecklist.pdf>

U.S. Department of Homeland Security, *Pandemic Influenza**Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources* 2006,

<http://www.flu.gov/planning-preparedness/business/cikrpandemicinfluenzaguide.pdf>

Luis Kun, *Protection of the Healthcare and Public Health Critical Infrastructure and Key Assets*, IEEE Engineering in Medicine and Biology Magazine, November/December 2008, ([https://www.hawaii.edu/csati/summit/Protection\_of\_The\_HC&PH\_Kun.pdf](https://www.hawaii.edu/csati/summit/Protection_of_The_HC%26PH_Kun.pdf)

U.S. Government Accountability Office, *Influenza Pandemic: Opportunities Exist to Address Critical Infrastructure Protection Challenges That Require Federal and Private Sector Coordination*,2007, <http://www.gao.gov/new.items/d0836.pdf>.

U.S. Government Accountability Office,*Influenza Pandemic: Lessons from the H1N1 Pandemic Should Be Incorporated into Future Planning*, 2011, <http://www.gao.gov/products/GAO-11-632>

National Infrastructure Advisory Council, *The Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States*, 2007,

<http://www.dhs.gov/xlibrary/assets/niac/niac-pandemic-wg_v8-011707.pdf>

North American Electricity Reliability Corporation, *High-Impact Low-Frequency Event Risk to the North American Bulk Power System*, 2010, <http://www.nerc.com/files/HILF.pdf> (Pandemic Influenza Section)

1. **Additional Recommended Reading:**

<https://www.osha.gov/Publications/influenza_pandemic.html>

The White House, *National Strategy for Pandemic Influenza*, 2005,

<http://www.flu.gov/planning-preparedness/federal/pandemic-influenza.pdf>

Congressional Research Service, *Banking and Financial Institution Continuity: Pandemic Flu, Terrorism, and Other Challenges*, May 2009, <http://www.fas.org/sgp/crs/misc/RL31873.pdf>. (Read parts applicable to pandemic influenza)

**Lesson 13 topic: collaborative case study presentations (part 1)**

**\*\*special activity: written case study is due to the instructor via e-mail at the beginning of class on lesson 14**.

**1. Lesson Goals/Objectives**:

* Provide the highlights and foster classroom discussion on critical infrastructure-focused emergent threat case studies and threat management recommendations.

**2. Discussion Topics**:

* Learner Team presentations.

**3. Required Reading**:

* As required for case study development and presentation.

**lesson 14 topic: collaborative case study presentations (part 2)**

**\*\*special activity: written case study is due to the instructor via e-mail by the beginning of class today**.

**1. Lesson Goals/Objectives**:

* Provide the highlights and foster classroom discussion on critical infrastructure-focused emergent threat case studies and threat management recommendations.

**2. Discussion Topics**:

* Team presentations.

**3. Required Reading**:

* As required for case study development and presentation.

**lesson 15 topic: understanding, planning for, and addressing long-term and enduring threats 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 the strategic choices that may impact our approach to critical infrastructure security and resilience 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 begin to happen now to adequately prepare for the future world of critical infrastructure security and resilience.

**2. Discussion Topics**:

* What can we predict about how the homeland security and critical infrastructure threat 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 major changes do you anticipate?
* What will the principal threats and challenges to critical infrastructure security and resilience 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?
* 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 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 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 threats?

**3. In-Class Exercise**: Learners will be assigned into teams to develop and informally present alternative scenarios regarding the critical infrastructure security and resilience operating and risk environments, as well as related issues and challenges.

**4. Required Reading**:

Mickey McCarter, *Future Homeland Security Threats Comprise Smaller Groups, Cybersecurity Vulnerabilities, Experts Say,* 2012,

<http://www.hstoday.us/single-article/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 Year2025,* 2012,

[*http://www.insidepolitics.org/brookingsreports/homeland\_security.pdf*](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/docs/Guarding-Our-Future.pdf.](http://www.toffler.com/docs/Guarding-Our-Future.pdf)

Toffler Associates, *Five Critical Threats to the Infrastructure of the Future,* 2008, [http://www.toffler.com/docs/Five-Critical-Infrastructure-Threats.pdf.](http://www.toffler.com/docs/Five-Critical-Infrastructure-Threats.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.](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>

Sam Powers, *The Threat of Cyberterrosim to Critical Infrastructures,* 2013,

<http://www.e-ir.info/2013/09/02/the-threat-of-cyberterrorism-to-critical-infrastructure/>

Rob Puentes, *Memo to the President: Invest in Infrastructure for Long-term Prosperity,*

Brookings Institution, Washington, D.C., 2009, [http://www.brookings.edu/papers/2009/0112\_prosperity\_memo.aspx.](http://www.brookings.edu/papers/2009/0112_prosperity_memo.aspx)