**Course Number: XXXX**

**Critical Infrastructure Security and Resilience: Sector Approaches and Cross-Sector Interdependencies**

**University of XXXXXX**

**Fall/Spring Semester 20XX**

**name of school:**

**department:**

**professor:**

Telephone Number:

Office Location:

Office Hours:

Email:

Website:

**course description/overview:**

The risk environment affecting our critical infrastructures comprises a diverse and complex 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 appropriately manage risk and enhance both security and resilience in the context of these complexities, government and industry partners have worked together for more than a decade to develop and implement a focused national approach and supporting plans and coordinating structures. This approach balances resilience with risk-informed prevention, protection, and preparedness activities to allow us to manage the most serious risks to our critical infrastructures, now and in the future. This effort continues with a reinvigorated focus under the new national guidance provided in Presidential Policy Directive 8 (PPD-8), “National Preparedness.”

Government agencies and private sector entities that share responsibility for critical infrastructure security and resilience represent a varied mix of authorities, capabilities, and resources. These actors also have unique concerns arising from the relative risks and the functional dependencies and interdependencies that characterize the infrastructure of concern within their individual purviews. These diverse factors result 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 is particularly true for those infrastructures that cross geopolitical and sector boundaries. 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 risk. This course will provide an in-depth look at these issues and the dynamic interplay between the various stakeholders engaged in the critical infrastructure security and resilience mission area.

This course is a 15-lesson graduate-level elective seminar providing a focus on critical infrastructure security and resilience from a sector-based perspective. It is designed to promote subject-matter understanding, critical analysis of issues, insight into senior leader decision-making, and an appreciation of the changing dynamics in the multidisciplinary field of critical infrastructure security and resilience. Specific areas of focus include: government-private sector policy approaches; risk assessment and management; performance measurement; dependencies and interdependencies; and incident management. The course also features a comprehensive practical examination of critical infrastructure sector stakeholder interaction and key subject-matter areas through in-class exercises, a collaborative critique project, and an interactive tabletop exercise focused on infrastructure interdependencies. These “hands-on” applications will reinforce knowledge and critical thinking skills gained throughout the course and help learners fully recognize the “whole of community” nature of critical infrastructure security and resilience within and across sectors. In terms of the 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 evolution of critical infrastructure security and resilience as a major policy area, including a look at the various strategies, frameworks, and plans that provide national-level guidance for this subject area. This includes discussion of the nexus between critical infrastructure security and resilience and the five mission area frameworks under PPD-8—prevention, protection, response, recovery, and mitigation. The course then turns to a review of the strategic context presented by the current and future risk environment, as well as the building blocks of critical infrastructure security and resilience: risk analysis and management, and partnering and information sharing. This discussion sets the stage for the next section of the course in which learners will assess, compare, and contrast the various approaches vis-à-vis security and resilience utilized within the various critical infrastructure sectors, including those that operate within a defined regulatory space and those that do not. Finally, the course will examine the nature of critical dependencies and interdependencies across the sectors, including a focus on organizational awareness and preparedness culture, supply chain security and cyber-related issues. This discussion will be enhanced by an interactive tabletop exercise that provides a deeper look at dependency/interdependency issues through the lens of an emergent threat and incident scenario impacting multiple critical sectors.

**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 (as Aligned to u.s. department of homeland security (dhs) core competencies):**

This course is designed to enable learners to:

**1. Be knowledgeable of the evolution of critical infrastructure security and resilience as a core homeland security policy area:**

* Course introduction and overview
* Discussion of framing principles and concepts
* Review of the roles and responsibilities of public and private sector critical infrastructure stakeholders
* Review of the historical evolution of critical infrastructure security and resilience as a national policy focus area, including overarching policy approaches and stakeholder implications
* Review of the core elements of the various national policies, strategies, plans, and reports that together provide the cornerstone for the U.S. approach to critical infrastructure security and resilience

**2. Understand the relationship between critical infrastructure security and resilience and the various mission area frameworks as defined in PPD-8:**

* National Prevention Framework
* National Protection Framework
* National Response Framework
* National Recovery Framework
* National Mitigation Framework

**3. Assess the 21st century risk environment and the implications it presents regarding critical infrastructure security and resilience:**

* Threats: terrorism, natural disasters and other naturally occurring phenomena, industrial accidents and technological failures, cyber attacks, and other emergencies
* Vulnerabilities (individual, facility/ node, and system level)
* Consequences (public health and safety, economic loss/disruption, continuity of government and essential services, etc.)
* Cyber risk
* Supply chain issues and dependencies/interdependencies.

**4. Be familiar with the basic building blocks of critical infrastructure security and resilience:**

* Risk analysis, risk mitigation, and performance measurement:
* Physical security
* Cybersecurity
* Insider Threats (including personnel surety)
* Resilience
* External connections
* Sector-specific considerations
* Partnership frameworks, information sharing processes/systems, and coordination/collaboration structures:
* Federal, State, local, tribal, territorial (SLTT), and private sector collaboration, coordination, and communication
* Critical infrastructure data collection, warehousing, and protection
* All-hazards information sharing
* Challenges and opportunities

**5. Understand and be able to demonstrate the practical application of critical infrastructure security and resilience in a dynamic risk and operating environment within and across the following interdependent sectors (which represent a subset of the critical sectors identified in the NIPP):**

* Agriculture and Food
* Chemical
* Communications
* Critical Manufacturing
* Defense Industrial Base
* Energy
* Financial Services
* Information Technology
* Healthcare and Public Health
* Transportation Systems
* Water

**6. Develop an advanced understanding of and practical familiarity with critical infrastructure sector interdependencies in the context of emergent threats and incidents through selected case studies and in-class exercises:**

* Aum Shinrikyo Tokyo Subway Attack (1995)
* 9/11 Attacks
* Anthrax Postal System Attacks (2001)
* Northeast Power Blackout 2003
* Madrid/London Transit Bombings (2004 and 2005)
* Hurricanes Katrina, Rita, and Wilma (2005)
* Mumbai Attack (2008)
* British Petroleum Gulf Coast Oil Spill (2010)
* Great East Japan Earthquake/ Tsunami/Fukushima Daiichi Reactor Disaster (2011)
* Superstorm Sandy (2012)
* Boston Marathon Bombing (2013)
* Ongoing Cyber Threats and Incidents

**delivery method/course requirements:**

Course delivery will be through mini-lectures, structured collaborative projects and in-class exercises, guest speakers, and interactive classroom discussions. 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), and independent external reviews (U.S. Government Accountability Office (GAO), Congressional Research Service (CRS), etc.). 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 25%

Collaborative Critique Project 40%

Oral Presentation 15%

Interdependencies Exercise 20%

(including player roles/responsibilities point paper)

Total 100%

**oral/written requirements:**

1. **Collaborative Critique Project + Oral Presentation (55%):**

Learners will work collaboratively in 2-person teams to develop and present a 20-25 page, section-by-section, critique of an assigned Sector Specific Plan under the National Infrastructure Protection Plan (NIPP) umbrella, with specific alternatives (policies, strategies, programs, technical solutions, etc.) provided for those areas in which they deem that the SSP falls short or could be improved. For template purposes, learners will follow the format in which the individual SSPs are structured.

Each team will present the highlights of its critique and alternative implementation approaches to the class during Lessons 14-15 using the format discussed above. This presentation should involve all team members and be no more than 30 minutes in length. **The completed written project deliverable must be submitted no later than the beginning of class on Lesson 14 for all project teams.**

**The instructor will make sector assignments and team pairings at the end of class on Lesson 4**.

1. **Critical Infrastructure Interdependencies Exercise (20%):**

Learners will participate in a role-based, interactive tabletop exercise highlighting the various dependencies/interdependencies between the critical sectors in the context of an emergent threat/incident. The exercise scenario simulates critical infrastructure-related preparations for, response to, and recovery from a Category 3 hurricane striking the Gulf Coast of the United States. The outline for this exercise is provided in **Attachment 1**. For exercise purposes, each learner will be assigned a role as a key government or private sector official with attendant critical infrastructure concerns and responsibilities (i.e., National Security Staff, Domestic Response Group member, Federal Sector Specific Agency lead, Federal Emergency Management Agency Response and Recovery official, state homeland security advisor/emergency manager, National Infrastructure Coordination Center director, Information Sharing and Analysis Center coordinator, Sector Coordinating Council chairperson, corporate security/emergency management director, etc.). The exercise will include three distinct phases: 1) an emerging threat phase, 2) an immediate response phase, and 3) a post-incident recovery phase.

In preparation for the exercise, **each learner will develop a short 2-3-page paper in bulleted, talking point format delineating his/her assigned role-based responsibilities corresponding to each phase of exercise play**, focused on infrastructure interdependencies issues as mapped against the National Mitigation, Response and Recovery Frameworks under PPD-8. The paper should also provide specific information regarding the relationship between the role being played and critical infrastructure dependencies/interdependencies concerns. **This paper will be submitted at the beginning of class on Lesson 13.** Individual learner roles for the exercise will be assigned by the instructor during class on **Lesson 5**.

1. **Expectations for In-Class Participation (25%):**

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 critique project, team oral presentation, and interdependencies exercise point paper. Ongoing dialogue with the instructor regarding project development, oral presentation preparation, and interdependencies exercise participation is highly encouraged.

**course textbooks:**

The following textbooks are identified as primary reading materials for the course. These textbooks will be supplemented by additional primary and suggested readings accessible on-line, with website addresses provided in the lesson description section that follows below.

Lewis, Ted G., ed. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, NJ: John Wiley & Sons, Inc., 2006.

Collins, Pamela A. and Ryan K. Baggett. *Homeland Security and Critical Infrastructure Protection* Santa Barbara: Praeger Security International, 2009.

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

**course outline**

**lesson 1 topic: course overview & review of critical infrastructure security and resilience as a national policy focus area**

**1. Lesson Goals/ Objectives:**

* Discuss the scope of the course, administrative requirements, instructional methodology, evaluation criteria, deliverables, and feedback processes.
* Review and discuss the evolution of critical infrastructure security and resilience as a national policy focus area.
* Review and discuss the various statutes and Presidential policy documents addressing critical infrastructure security and resilience, including general principles and their application to strategy development and planning.
* Develop a practical understanding of how critical infrastructure security and resilience policies and plans have changed over time as a function of the “all-hazards” risk environment.
* Review the various component elements of the NIPP (general principles, stakeholder roles and responsibilities, governance & partnerships, information sharing, risk analysis and management, etc.) and discuss examples of how these component elements relate to one another.

**2. Discussion Topics:**

* 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 across sectors and governmental jurisdictions regarding critical infrastructure security and resilience?
* Why does critical infrastructure security and resilience represent such a challenge within and across governmental jurisdictions and sectors?
* How would you characterize the evolution of U.S. critical infrastructure policy over time? How did we get where we are today? Are we where we need to be?
* What are the general principles we typically associate with critical infrastructure security and resilience in the U.S. context?
* What are the differences between the various Presidential policies focused on critical infrastructure security and resilience over the last 15 years?
* 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 steady state preparedness, collaboration, and incident management operations?
* How has the Nation’s approach to critical infrastructure preparedness and planning changed over time and with regard to specific threats and hazards (provide specific examples)?
* What is the role of the National Security Staff in the critical infrastructure security and resilience arena? How does it affect national policy?
* How does the U.S. Congress view the critical infrastructure security and resilience policy area? Does legislation clarify or complicate the critical infrastructure security and resilience mission space?
* What are the key elements of critical infrastructure security and resilience as discussed in the NIPP? How do these key elements relate to/interact with one another?
* What are the key elements of PPD 21 and the Executive Order on Improving Critical Infrastructure Cybersecurity and how do these documents contribute to the evolution of the critical infrastructure security and resilience mission area?
* What are the key recommendations contained in the 2010 National Infrastructure Advisory Council Report, “A Framework for Establishing Critical Infrastructure Resilience Goals?” Do you concur with these recommendations? Why or why not?

1. **Required Reading**:

Lewis,Chapters 1 and 2.

Collins and Baggett, Chapters 1-3.

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: U.S. Department of Homeland Security, 2013. 1-10, 13-14. <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.

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, 78 Fed. Reg. 11739 (2013) (Improving Cybersecurity Critical Infrastructure).

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

Moteff, John D., Cong. Research Service*,* RL 30153,Critical Infrastructures: Background, Policy, and Implementation(2014).<http://fas.org/sgp/crs/homesec/RL30153.pdf>.

Moteff, John D., Cong. Research Service, R42683, *Critical Infrastructure Resilience: The Evolution of Policies and Programs and Issues for Congress* (2012). <http://www.fas.org/sgp/crs/homesec/R42683.pdf>

U.S. Department of Homeland Security. *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*. Washington, DC: U.S. Department of Homeland Security, 2014. <http://www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.pdf>.

McNeill, Jena Baker and Richard Weitz. *How to Fix Homeland Security Critical Infrastructure Protection Plans: A Guide for Congress*. Washington, DC: The Heritage Foundation, 2010. <http://www.heritage.org/research/reports/2010/04/how-to-fix-homeland-security-critical-infrastructure-protection-plans-a-guide-for-congress>

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

Whitaker, Alan G., Shannon A. Brown, Frederick C. Smith, and Elizabeth McKune. *The National Security Policy Process: The National Security Council and Interagency System*. Washington, DC: Industrial College of the Armed Forces, National Defense University, U.S. Department of Defense,2011.

<http://www.virginia.edu/cnsl/pdf/national-security-policy-process-2011.pdf>

1. **Additional Recommended Reading:**

Exec. Order No. 13010*,* 3 C.F.R. 13010(1996) (Critical Infrastructure Protection).

<http://www.fas.org/irp/offdocs/eo13010.htm>.

Presidential Decision Directive-63*,* 63 Fed. Reg. 41804 (1998)(Critical Infrastructure Protection). <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

Homeland Security Presidential Directive-7,

*Critical Infrastructure Identification, Prioritization and Protection* (2003), <http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1>.

Homeland Security Act, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

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

White House. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC: White House,2003.<http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.

White House. *National Security Strategy*. Washington, DC: White House,2010.

<http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>

Marsh, Robert T. *Critical Foundations: Protecting America’s Infrastructures*. Arlington, VA: Marshall Institute,1997. <http://www.marshall.org/article.php?id=65>.

**lesson 2 topic: critical infrastructure security and resilience and the national prevention and protection frameworks**

**1. Lesson Goals/Objectives**:

* Define and describe the concepts of “prevention,” “protection,” and “resilience,” as they relate to critical infrastructure security and resilience from both a government and an industry perspective.
* Define and describe the major elements of PPD-8 and the PPD-8 implementation process, including the National Preparedness Goal, National Preparedness System, and Core Capabilities.
* Articulate the nexus between PPD-8 implementation and critical infrastructure security and resilience, with a focus on prevention and protection core capability development and delivery.
* Articulate the nexus between the National Prevention and Protection Frameworks and the critical infrastructure security and resilience community, including the “Whole Community” approach described in the National Preparedness Goal.
* Critique the various approaches to developing and implementing critical infrastructure prevention and protection strategies and initiatives at the Federal, State, local, tribal, and territorial level, as well as across the private sector.
* Define and explain the concept of “community resilience” as it relates to critical infrastructure security and resilience planning.

**2. Discussion Topics**:

* How do the concepts of “security” and “resilience” relate to one another, and how do they apply in the context of critical infrastructure security and resilience planning? From a government perspective? From an industry perspective?
* What are the general principles and concepts associated with resilience as currently applied by government and industry?
* How do we achieve an appropriate balance between prevention, protection, and resilience in the context of critical infrastructure security and resilience planning?
* What are the similarities and differences between “critical infrastructure resilience” and “community resilience?”
* What are the major recommendations of the 2009 National Infrastructure Advisory Council (NIAC) Report regarding resilience? Do you concur with them? If not, what would be your recommendations?
* What are the major concepts identified within PPD-8? What are the major elements that comprise PPD-8 implementation?
* How does critical infrastructure and resilience factor into the National Preparedness Goal? The National Preparedness System? The “Whole Community” approach?
* How do the Core Capabilities that form part of the National Preparedness System relate to critical infrastructure security and resilience?
* How does critical infrastructure security and resilience relate to the National Prevention and Protection Frameworks? How do these frameworks intersect/inter-relate with one another? Are there gaps? Inconsistencies? Major differences?
* What are the core capabilities discussed in the National Prevention and Protection Frameworks that are most relevant to critical infrastructure security and resilience? How would they best be delivered?
* How do the National Prevention and Protection Frameworks relate to the NIPP? Are there any inconsistencies?
* How does industry plan for the critical infrastructure security and resilience mission? How does business continuity planning relate to critical infrastructure security and resilience? How do the government and private sectors interact in the critical infrastructure security and resilience and business continuity planning processes?
* How does the DHS Regional Resilience Awareness Program (RRAP) contribute to community resilience?

1. **In-class exercise:** The class will be divided into two teams, each representing one of the two National Mission Area Frameworks discussed in this lesson. The instructor will conduct a high-level “walk through” of various malicious actor scenarios. Each team will respond to questions posed by the instructor based upon the perspective corresponding to the Framework they have been assigned.

**4. Required Reading**:

Gov’t Accountability Office, GAO-10-296, Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience (2010). <http://www.gao.gov/new.items/d10296.pdf>.

Kennedy, Jim. “Critical Infrastructure Protection is All About Operational Resilience.” *Continuity Central* (November 17, 2006). <http://www.continuitycentral.com/feature0413.htm>.

National Infrastructure Advisory Council. *Critical Infrastructure Resilience Final Report and Recommendations*. Arlington, VA: National Infrastructure Advisory Council, 2009.

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

George Mason University, The Center for Infrastructure Protection and Homeland Security. *The CIP Report*. 12, no. 6 (December 2013).

<http://cip.gmu.edu/wp-content/uploads/2014/01/December-2013_Resilience.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security. *The CIP Report*. 12, no. 7 (January 2014). <http://cip.gmu.edu/wp-content/uploads/2013/06/January-2014_Resilience.pdf>.

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

“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>

U.S. Department of Homeland Security. *National Prevention Framework*. Washington, DC: U.S. Department of Homeland Security, 2013. <http://www.fema.gov/media-library-data/20130726-1913-25045-6071/final_national_prevention_framework_20130501.pdf>

U.S. Department of Homeland Security. *National Protection Framework*. (Not released as of July 2014)

“Regional Resiliency Assessment Program.” *U.S. Department of Homeland Security*. <http://www.dhs.gov/regional-resiliency-assessment-program>

**5. Additional Recommended Reading:**

Gov’t Accountability Office, GAO-13-11, An Implementation Strategy Could Advance DHS’s Coordination of Resilience Efforts Across Ports and Other Infrastructure (2012). <http://www.gao.gov/assets/650/649705.pdf>

The Infrastructure Security Partnership. *Regional Disaster Resilience Guide*. Alexandria, VA: TISP, 2008. <http://www.tisp.org/index.cfm?cdid=11493&pid=10261> (**general review only**).

Hardenbrook, Brandon J. “The Need for a Policy Framework to Develop Disaster Resilient Regions.” *Journal of Hameland Security and Emergency Management* 2, no. 3 (2005). <http://www.bepress.com/jhsem/vol2/iss3/2/>.

“Critical Infrastructure Protection Partnerships and Information Sharing.” *U.S. Department of Homeland Security*. <http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing>

**lesson 3 topic: critical infrastructure security and resilience and the national response, recovery and mitigation frameworks**

**1. Lesson Goals/Objectives**:

* Articulate the nexus between PPD-8 implementation and critical infrastructure security and resilience, with a focus on response, recovery, and mitigation core capability development and delivery.
* Articulate the nexus between the National Response, Recovery, and Mitigation Frameworks and the critical infrastructure security and resilience community, including the “Whole Community” approach described in the National Preparedness Goal.
* Explain how the National Response, Recovery, and Mitigation Frameworks relate to the NIPP and its Sector Specific Plans.

**2. Discussion Topics**:

* How does critical infrastructure security and resilience factor into the National Preparedness Goal? The National Preparedness System? The “Whole Community” approach?
* How do the Core Capabilities that form part of the National Preparedness System relate to critical infrastructure security and resilience?
* How do the National Response, Recovery, and Mitigation Frameworks relate to the National Prevention and Protection Frameworks discussed in the last lesson?
* How is the critical infrastructure security and resilience focus area accounted for in the National Response, Recovery, and Mitigation Frameworks? How do these frameworks intersect/inter-relate with one another with respect to critical infrastructure equities? Are there gaps? Inconsistencies? Major differences?
* What are the differences between “protection” and “mitigation” in the context of PPD-8?
* What are the core capabilities discussed in the National Response, Recovery, and Mitigation Frameworks that are most relevant to critical infrastructure security and resilience? How and by whom would they best be delivered?
* How do the National Response, Recovery, and Mitigation Frameworks relate to the NIPP? Are there any inconsistencies?
* How does industry plan for critical infrastructure response and recovery? How do industry and government work together in this area according to the National Frameworks? How are the various stakeholder needs identified and addressed and how is collaboration achieved? Are there any disconnects?
* What are the major challenges related to public-private sector collaboration in disaster recovery from a critical infrastructure perspective? Are these challenges exacerbated in the context of Internet infrastructure? Why or why not?
* How does the NIMSAT Report on public-private partnership address the issues surrounding the establishment, interaction, resourcing, and sustainment of such partnerships?

1. **In-class Exercise:** The class will be divided into three teams, each representing one of the three National Mission Area Frameworks discussed in this lesson. The instructor will conduct a high-level “walk through” of various manmade and natural disaster scenarios. Each team will respond to questions posed by the instructor based upon the perspective corresponding to the Framework they have been assigned.

**4. Required Reading**:

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

“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>

U.S. Department of Homeland Security. *National Response Framework*. Washington, DC: U.S. Department of Homeland Security, 2013. <http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf>

U.S. Federal Emergency Management Agency. *National Disaster Recovery Framework: Strengthening Disaster Recovery for the Nation*. Washington, DC: FEMA, 2011. <http://www.fema.gov/pdf/recoveryframework/ndrf.pdf>

U.S. Department of Homeland Security. *National Mitigation Framework*. Washington, DC: U.S. Department of Homeland Security, 2013. <http://www.fema.gov/media-library-data/20130726-1914-25045-9956/final_national_mitigation_framework_20130501.pdf>

*Compendium of Public-Private Partnerships for Emergency Management*. Lafayette, LA: NIMSAT Institute, University of Louisiana at Lafayette, 2012. <http://www.padres-ppp.org/NimsatPPP/resources/Final%20PPP%20Report_101812.pdf>

George Mason University, Center for Infrastructure Protection and Homeland Security. *The CIP Report* 11, no. 4 (October 2012). <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/THeCIPReport_October2012_InfrastructureRecovery.pdf>

U.S. Government Accounting Office, GAO-08-212T, Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan(2007). <http://www.gao.gov/new.items/d08212t.pdf>.

**5. Additional Recommended Reading:**

U.S. Gov’t Accountability Office, GAO-08-36, 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>.

**lesson 4 topic: assessing critical infrastructure sector risk in an interdependent world**

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

**1. Lesson Goals/Objectives**:

* Identify, define, and develop an advanced understanding of the major elements of risk in the context of critical infrastructure sector-level planning: threats, vulnerabilities, and consequences.
* Explain how the elements of risk relate to the human, physical, and cyber aspects of critical infrastructure security and resilience at the sector level.
* Critique the DHS strategic risk assessment process, as well as how other government and private sector critical infrastructure stakeholders view and evaluate risk.
* Identify and assess the complexities regarding critical infrastructure dependencies and interdependencies as they relate to risk.
* Explain how risk drives critical infrastructure risk management strategies, plans, and resource investment at the sector level.
* Identify and describe the challenges associated with critical infrastructure sector security and resilience planning in the potential future risk environment.

**2. Discussion Topics**:

* How are the major elements of risk quantified to support risk management decisions in the context of critical infrastructure?
* How has the nature of the risks to our critical infrastructure sectors evolved over time? How does this risk vary among the sectors?
* How does the fractured structure of responsibility and accountability in the critical infrastructure security and resilience community area play out vis-a-vis the principal threats we face?
* What are the principal challenges we face in ensuring the security and resilience of our critical infrastructure at the sector level in light of these risks?
* How do PPD 21 and the Obama Administration’s Executive Order on Improving Critical Infrastructure Cybersecurity address the integration of cyber and physical risk analysis pertaining to critical infrastructure?
* How does the NIPP address the subject of risk? How are sector-level risks prioritized within the NIPP framework? Other government frameworks? Business continuity planning frameworks?
* Does the FEMA Threat Hazard Information Risk Assessment (THIRA) process account for critical infrastructure risk? Does it account for such risk at a sector level?
* How do the human, physical, and cyber dimensions of critical infrastructure security and resilience relate to the concept of risk at the sector level?
* How does the Federal government assess risk and communicate the results of the risk assessment process to other critical infrastructure stakeholders at the sector level? Do these other players have a role to play in government risk assessment processes and programs?
* How does risk management relate to sector-level strategies, planning, and resource investments in the critical infrastructure security and resilience mission area?
* How do we calculate risk across threat/hazard types? Across jurisdictions? Across sectors?
* What are the advantages/disadvantages of the various approaches to risk as practiced within the NIPP Partnership Framework?
* Is the voluntary approach working to produce a measurable increase in security in those sectors in which regulation is not operative?
* How does the concept of incentives play within a voluntary security and preparedness construct?

**3. Required Reading**:

Collins and Baggett, Chapters 5, 13, and 15.

Lewis, Chapter 4, pp. 71-73; Chapter 5, pp. 107-110; and Chapter 13.

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: U.S. Department of Homeland Security, 2013. 15-20, 23-25. <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.

Moteff, John, Claudia Copeland, and John Fischer, Cong. Research Service, RL 31556, What Makes Infrastructure Critical? (2002),

<http://www.libertysecurity.org/IMG/pdf/CRS_Report_-_What_makes_an_Infrastructure_Critical_-_30.08.2002.pdf>.

Parfomak, Paul W., Cong. Research Service*,* RL 33206,Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options (2006).

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

George Mason University, Critical Infrastructure Protection Program. “The Meaning of Vulnerability in the Context of Critical Infrastructure Protection.” in *Critical Infrastructure Protection: Elements of Risk.* Arlington, VA: George Mason University, 2007. <http://cip.gmu.edu/wp-content/uploads/2014/03/ElementsofRiskMonograph.pdf>.

Gov’t Accountability Office, GAO-12-378, DHS Could Better Manage Security Surveys and Vulnerability Assessments (2012). <http://www.gao.gov/assets/600/591292.pdf>

National Research Council. Review of the Department of Homeland Security's Approach to Risk Analysis. Washington, DC: The National Academies Press, 2010. <http://www.nap.edu/catalog.php?record_id=12972>.

Jackson, Brian and David Frelinger. *Emerging Threats and Security Planning*. Santa Monica, CA: RAND Corp., 2009. <http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP256.pdf>.

National Research Council. Sustainable Critical Infrastructure Systems: A Framework for Meeting 21st Century Imperatives. Washington, DC: The National Academies Press, 2009. <http://www.nap.edu/openbook.php?record_id=12638&page=R1>.

Prieto, Bob. *Infrastructure Resiliency: Do We Have the Focus Right?* Alexandria, VA: The Infrastructure Security Partnership, 2009. <http://www.tisp.org/index.cfm?cdid=11838&pid=10261>.

Jackson, Brian. *Marrying Prevention and Resiliency.* Santa Monica, CA: RAND Corp., 2008. <http://www.rand.org/pubs/occasional_papers/2008/RAND_OP236.pdf>.

Orszag, Peter R. *Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentives.* Congressional Testimony (2003). <http://www.brookings.edu/~/media/Files/rc/testimonies/2003/0904healthcare_orszag/20030904.pdf>.

1. **Recommended Additional Reading:**

“Comprehensive Preparedness Guide 201: Threat and Hazard Identification and Risk Assessment Guide.” *FEMA* (August 29, 2013). <http://www.fema.gov/library/viewRecord.do?fromSearch=fromsearch&id=5823>

U.S. Gov’t Accountability Office, GAO-08-904T, Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security (2008), <http://www.gao.gov/products/GAO-08-904T>.

Haimes, Yacov Y. “On the Complex Definition of Risk: A Systems-Based Approach.” *Risk Analysis* 29, no. 12 (2009): 1647- 54. <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2009.01310.x/pdf>.

**lesson 5 topic: the sector approach to organizing, partnering, and sharing information for critical infrastructure security and resilience**

**\*\*Special Activity: The instructor will assign individual learner roles for the critical infrastructure interdependencies exercise at the end of class**.

**1. Lesson Goals/Objectives**:

* Review and discuss the sector-level structures, processes, and coordinating mechanisms associated with the NIPP Partnership Model.
* Describe the nature of collaborative interaction between the Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), and Regional Consortium Coordinating Council (RCCC) under the NIPP framework.
* Identify and discuss the various methods, processes, and systems that the various sector partners use to share information with one another.
* Identify and discuss the major elements of the Critical Infrastructure Information Act of 2002 and the Protected Critical Infrastructure Information Program.
* Evaluate the ongoing challenges and barriers to information sharing and collaboration that exist between the various levels of government and the private sector.
* Critique the processes and systems through which critical infrastructure and resilience-related information is collected, warehoused, protected, and exchanged between various levels of government and the private sector.

**2. Discussion Topics**:

* What are the key elements of the NIPP partnership model? How are these elements captured in key critical infrastructure security and resilience strategies and plans?
* How does one go about the process of building a government-private partnership network or coalition for critical infrastructure security and resilience purposes?
* How are the critical infrastructure sectors organized to accomplish the critical infrastructure security and resilience mission at the sector and sub-sector levels? What is their “motivation” regarding their role in executing this mission?
* What is the Critical Infrastructure Partnership Advisory Council (CIPAC)? How does the CIPAC structure facilitate strategy and plan development within the critical infrastructure security and resilience community?
* How do the various elements of the NIPP Partnership Model interact with one another (“steady state” and during emergent threats and incident scenarios)? How effective is this model in achieving the necessary level and quality of information sharing required to execute the critical infrastructure security and resilience mission?
* What are the major elements of the Critical Infrastructure Information Act of 2002 and the Protected Critical Infrastructure Information Program? How do they afford security to security information provided on a voluntary basis to the government by the private sector?
* How do PPD 21 and the Obama Administration’s Executive Order on Improving Critical Infrastructure Cybersecurity impact critical infrastructure information sharing?
* What are the Information Sharing and Analysis Centers (ISACs)? How do they interact with government? What role do they play in critical infrastructure security and resilience planning and incident management?
* What are the principal barriers to sharing information proactively and comprehensively between government and industry at all levels of the NIPPpartnership framework?
* What are the principal types and sources of information that support the critical infrastructure security and resilience mission?
* What are the key processes and systems used to share critical infrastructure security and resilience-related data at the sector level, including intelligence-related information, among the various stakeholders nationally, regionally, and locally?
* How is classified national security information shared between government and industry? How and from whom does industry receive terrorism-related information?
* How do government and industry work together to protect sensitive information? Are there areas for improvement?
* What are the roles and responsibilities of DHS; FBI; and the State, local and regional fusion centers regarding critical infrastructure security and resilience information sharing and analysis?
* How is information and intelligence that originates from multiple distributed sources compiled and de-conflicted?
* How does information sharing factor into critical infrastructure security and resilience strategy and planning efforts?

**3. Required Reading**:

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: U.S. Department of Homeland Security, 2013. 10-12, App’x A. <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.

Eckert, Sue. *Protecting Critical Infrastructure: The Role of the Private Sector*. Pittsburgh: Ridgway Center, 2006. <http://www.ridgway.pitt.edu/LinkClick.aspx?fileticket=Bezaq7AdjxA%3D&tabid=233>.

“State and Major Urban Area Fusion Centers.” *U.S. Department of Homeland Security* (Last visited July 3, 2014).

<http://www.dhs.gov/files/programs/gc_1156877184684.shtm>.

*The Future of Fusion Centers: Potential Promise and Dangers*, *Before the Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment*, 111th Cong.(2009) (testimony of Robert Riegle, Director of the State and Local Program Office, Office of Intelligence and Analysis). <http://www.dhs.gov/ynews/testimony/testimony_1238597287040.shtm>.

ISAC Council. *A Policy Framework for the ISAC Community* (2004).

<http://www.isaccouncil.org/images/Policy_Framework_for_ISAC_Community_013104.pdf>.

ISAC Council. *The Role of ISACs in Private/Public Sector CIP* (2009).

http://www.isaccouncil.org/images/ISAC\_Role\_in\_CIP.pdf

“Information Sharing and the Private Sector.” *Information Sharing Environment*. <http://ise.gov/sharing-private-sector>

“Information Sharing Environment.” IT Law Wiki (Last Visited July 3, 2014).

<http://itlaw.wikia.com/wiki/Information_Sharing_Environment>.

“The Homeland Security Information Network.” *U.S. Department of Homeland Security* (Last visited July 3, 2014).<http://www.dhs.gov/homeland-security-information-network>

“Information Sharing: A Vital Resource for a Shared National Mission to Protect Critical Infrastructure.” *U.S. Department of Homeland Security* (Last visited July 3, 2014). <http://www.dhs.gov/information-sharing-vital-resource-shared-national-mission-protect-critical-infrastructure>

“Building Resilience through Public-Private Partnerships: Progress Report.” (January 2012).

<http://www.fema.gov/pdf/privatesector/building_ppp_report.pdf>.

Critical Infrastructure Information Act of 2002, 6 U.S.C. §§131 et seq.

Procedures for Handling Critical Infrastructure Information, 6 C.F.R. pt. 29 (2006).

<http://www.dhs.gov/sites/default/files/publications/pcii_final_rule_federal_register9-1-06-2_508.pdf>.

**4. Recommend Additional Reading**:

White House. *National Strategy for Information Sharing*. Washington, DC: White House, 2007.

<http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html>.

“Critical Infrastructure Partnerships.” *Critical Infrastructure Resource Center, U.S. Department of Homeland Security*.

<http://training.fema.gov/EMIWeb/IS/IS860b/CIRC/CIKRpartnerships.htm>.

**lesson 6 topic: sector profiles: information technology, communications and Financial Services**

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

**1. Lesson Goals/Objectives**:

* Describe the sector’s operational profile, composite make-up, major critical infrastructure dependencies and interdependencies, and goals and objectives.
* Describe the sector’s risk profile and evaluate the sector’s approach to risk assessment, risk management, performance measurement, and incident management.
* Explain the PPD-8 core capabilities relevant to the sector and how they are delivered.
* Assess the sector’s regulatory profile (if applicable), as well as the strengths and limitations of regulation as a means to promote critical infrastructure security and resilience within the sector.
* Critique the various policies, plans, and programs in place to promote critical infrastructure security and resilience within the sector.

**2. Discussion Topics**:

* How is the sector organized to facilitate critical infrastructure security and resilience? Who are the key players? What are the key authorities that can be used to facilitate security and resilience within the sector?
* What are the sector’s goals and objectives relative to security and resilience?
* How do government and industry interact to promote critical infrastructure security and resilience within the sector? To support incident management activities? What formal coordination/collaboration structures/mechanisms are in place?
* How is information pertinent to critical infrastructure security and resilience shared and protected within the sector? What are the principal information sharing mechanisms utilized at the sector level? Are these effective? Do they need to be enhanced?
* Discuss the sector’s risk profile. What are the principal threats and hazards faced by the sector? What are the sector’s principal vulnerabilities or areas of concern from a security and resilience standpoint?
* What is the sector’s approach to risk assessment and risk management? How is performance measured and how is change effected based on areas where improvement is required?
* How does the sector approach the issue of cyber security? How do government and industry interact to jointly address cyber risk within the sector?
* What are the sector’s major dependencies and interdependencies from a security and resilience standpoint? How are dependencies/interdependencies issues identified and addressed within the sector?
* Which PPD-8 core capabilities are most relevant to the sector and how are they delivered? What work remains to be done in this area?
* Is the sector regulated from a security and resilience standpoint? If so, what are the major components of the regulatory framework? Is the existing regulatory framework effective, or does it need to be enhanced in some way?
* How is the sector postured to support emergent threat and incident management activities?
* Discuss the various policies, plans, and programs in place to promote critical infrastructure security and resilience within the sector. Are they effective? How could they be improved?
* How might PPD 21 and the Obama Administration’s Executive Order on Improving Critical Infrastructure Cybersecurity impact information sharing within the sectors studied in this lesson?

**3. In-class Activity**: For this lesson, the class will be broken down into 3 teams. Each team will be assigned readings corresponding to one of the three sectors studied in this lesson. Each team will be prepared to discuss their sector’s operational and risk profiles, the sector approach to risk assessment and management, sector information sharing mechanisms, etc. In turn, the instructor will facilitate a discussion of the differences and commonalities, as well as the strengths and weaknesses of the various sector approaches. The instructor will also facilitate a comparative discussion of regulatory regimes, where they exist, as well as PPD-8 capabilities delivery within the sectors.

**4. Required Reading**:

General Reading (To be completed by all learners):

Collins and Baggett, Chapter 10.

Lewis, Chapter 8, pp. 223-244 and Chapter 14, pp. 429-440, 454-459.

Hentea, Mariana. *Improving Security for SCADA Control Systems*, (2008),

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

Gov’t Accountability Office, GAO-12-92, Cybersecurity Guidance is Available, but More Could be Done to Promote its Use (2011), <http://www.gao.gov/products/GAO-12-92>

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg, MD: Nationa Institute of Standards and Technology (2014).<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

IT Sector:

<http://www.hsdl.org/?view&did=7899> (Information Technology Sector Specific Plan)

<http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/infoTech1.htm> (Understanding the Information Technology Sector)

<http://www.it-scc.org/>

<http://www.it-scc.org/about/goals.php>

<https://www.it-isac.org/>

Communications Sector:

<http://www.dhs.gov/sector-specific-plans> (Communications Sector Specific Plan)

[http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/communications1.htm](http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/communications1.htm%20)  (Understanding the Communications Sector)

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

George Mason University, Center for Infrastructure Protection and Homeland Security. *The CIP Report* 11, no. 5 (November 2011). http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/TheCIPReport\_November-2012\_CommunicationsSector.pdf

Financial Services Sector:

<http://www.dhs.gov/sector-specific-plans> (Financial Services Sector Specific Plan)

<http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/bank1.htm> (Understanding the Financial Services Sector)

<http://www.fsisac.com/>

<http://www.availabilitydigest.com/public_articles/0710/fs-isac.pdf> (Financial Services Sector ISAC)

George Mason University, Center for Infrastructure Protection and Homeland Security. *The CIP Report 8*, no. 8 (February 2010). <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_February2010_BankingandFinanceSector.pdf>

Weiss, N. Eric, Cong. Research Service, RL 31873, Banking and Financial Institution Continuity: Pandemic Flu, Terrorism, and Other Challenges (2009). <http://www.fas.org/sgp/crs/misc/RL31873.pdf>.

**5. Additional Recommended Reading:**

<http://www.infosecisland.com/blogview/4291-DHS-Cyber-Security-Resources-Catalog.html> (DHS Cyber Resources Catalog)

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

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

U.S. Gov’t Accountability Office, GAO-10-834T, *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, Center for Infrastructure Protection and Homeland Security. *The CIP Report* 7, no. 8 (February 2009). <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_February2009_SCADA.pdf>.

**lesson 7 topic: sector profiles: energy and chemical and hazardous materials**

**1. Lesson Goals/Objectives**:

* Describe the sector’s operational profile, composite make-up, major critical infrastructure dependencies and interdependencies, and goals and objectives.
* Describe the sector’s risk profile and evaluate the sector’s approach to risk assessment, risk management, performance measurement, and incident management.
* Explain the PPD-8 core capabilities relevant to the sector and how they are delivered.
* Assess the sector’s regulatory profile (if applicable), as well as the strengths and limitations of regulation as a means to promote critical infrastructure security and resilience within the sector.
* Critique the various policies, plans, and programs in place to promote critical infrastructure security and resilience within the sector.

**2. Discussion Topics**:

* How is the sector organized to facilitate critical infrastructure security and resilience? Who are the key players? What are the key authorities that can be used to facilitate security and resilience within the sector?
* What are the sector’s goals and objectives relative to security and resilience?
* How do government and industry interact to promote critical infrastructure security and resilience within the sector? To support incident management activities? What formal coordination/collaboration structures/mechanisms are in place?
* How is information pertinent to critical infrastructure security and resilience shared and protected within the sector? What are the principal information sharing mechanisms utilized at the sector level? Are these effective? Do they need to be enhanced?
* How might PPD 21 and the Obama Administration’s Executive Order on Improving Critical Infrastructure Cybersecurity impact information sharing within the sectors studied in this lesson?
* Discuss the sector’s risk profile. What are the principal threats and hazards faced by the sector? What are the sector’s principal vulnerabilities or areas of concern from a security and resilience standpoint?
* What is the sector’s approach to risk assessment and risk management? How is performance measured and how is change effected based on areas where improvement is required?
* How does the sector approach the issue of cyber security? How do government and industry interact to jointly address cyber risk within the sector?
* What are the sector’s major dependencies and interdependencies from a security and resilience standpoint? How are dependencies/interdependencies issues identified and addressed within the sector?
* Which PPD-8 core capabilities are most relevant to the sector and how are they delivered? What work remains to be done in this area?
* Is the sector regulated from a security and resilience standpoint? If so, what are the major components of the regulatory framework(s) and how would you characterize the relationship between the regulator and the regulated party? Is/are the existing regulatory framework(s) effective, or does it (they) need to be enhanced in some way? How does the government-industry regulatory relationship affect the planning and performance measurement processes?
* Is there one or more model of regulation that stands out as more effective than the others within the sectors studied in this lesson? If so, why?
* What were some of the key impacts resulting from the deregulation of the Energy Sector? What was the motive behind this deregulation? Who has responsibility for risk mitigation within the Energy Sector? How is the sector postured to support emergent threat and incident management activities?
* Discuss the various policies, plans, and programs in place to promote critical infrastructure security and resilience within the sector. Are they effective? How could they be improved?
* Should cybersecurity be regulated within and across the critical sectors? Is cybersecurity regulation effective within the electricity sector?

**3. In-class Activity**: For this lesson, the class will be broken down into 2 teams. Each team will be assigned readings corresponding to one of the two sectors studied in this lesson. Each team will be prepared to discuss their sector’s operational and risk profiles, the sector approach to risk assessment and management, sector information sharing mechanisms, etc. In turn, the instructor will facilitate a discussion of the differences and commonalities, as well as the strengths and weaknesses of the various approaches. The instructor will also facilitate a comparative discussion of regulatory regimes, where they exist, as well as PPD-8 capabilities delivery within the sectors.

**4. Required Reading**:

Collins and Baggett, Chapters 6, 7, and 9.

<http://training.fema.gov/EMIWeb/IS/IS860b/CIRC/energy1.htm> (Understanding the Energy Sector)

<http://www.dhs.gov/critical-infrastructure-sectors> (Energy and Chemical and Hazardous Materials)

Onoda, Yusuke. *Energy Deregulation in the United States and Japan.* Cambridge, MA: Program on U.S.-Japan Relations, Harvard University,2007. See Chapter 2. <http://dev.wcfia.harvard.edu/us-japan/research/pdf/07-12.Onoda.pdf>.

<http://www.nerc.com/page.php?cid=6%7C69> (NERC critical infrastructure protection)

<http://www.esisac.com/SitePages/Home.aspx> (Information Sharing)

North American Electricity Reliability Corporation. *Integrated Bulk Power System Risk Assessment Concepts*. Washington, DC: North American Electricity Reliability Corporation, 2012. <http://www.nerc.com/docs/pc/rmwg/Integrated_Bulk_Power_System_Risk_Assessment_Concepts_Final.pdf>

George Mason University, Center for Infrastructure Protection and Homeland Security. *The CIP Report* 11, no. 2 (August 2012). <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/TheCIPReport_August2012_SmartGrid.pdf>

North American Electricity Reliability Corporation. *High-Impact Low-Frequency Event Risk to the North American Bulk Power System*. Washington, DC: North American Electricity Reliability Corporation, 2010. <http://www.nerc.com/pa/CI/Resources/Documents/HILF_Report.pdf>.

Idaho National Laboratory. *Vulnerability Analysis of Energy Delivery Control Systems*. Idaho Falls: Idaho National Laboratory, 2011).

<http://energy.gov/sites/prod/files/Vulnerability%20Analysis%20of%20Energy%20Delivery%20Control%20Systems.pdf>

U.S Department of Energy. *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. Washington, DC: U.S. Department of Energy, 2011. <http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf>

<http://www.nerc.com/page.php?cid=2%7C20> (Cybersecurity regulatory standards)

<http://training.fema.gov/EMIWeb/IS/IS860b/CIRC/chem1.htm>. (Understanding the Chemical Sector)

<http://www.chemicalcybersecurity.org/About/Chemical-Sector-Coordinating-Council.html>

U.S. Department of Homeland Security. *Chemical Sector Security Awareness Guide*. Washington, DC: U.S. Department of Homeland Security, 2010. <http://www.socma.com/assets/file/socma1/pdffiles/gr_pdf_files/dhs_chemical_sector_guide_final.pdf>

<http://www.dhs.gov/critical-infrastructure-chemical-security> (Chemical Facility Antiterrorism Standards Program Website)

U.S. Department of Homeland Security. *Chemical Facility Antiterrorism Standards: Final*. Washington, DC: U.S. Department of Homeland Security, 2007. <http://www.dhs.gov/files/laws/gc_1166796969417.shtm>.

Maritime Transportation Security Act of 2002, Pub. L. No. 107-295.<http://www.gpo.gov/fdsys/pkg/PLAW-107publ295/content-detail.html>.

Chemical Secotr Roadmap Working Group. *Roadmap to Secure Control Systems in the Chemical Sector*. Washington, DC: U.S. Department of Homeland Security, 2009. <http://scadahacker.com/library/Documents/Roadmaps/Roadmap%20to%20Secure%20Control%20Systems%20in%20the%20Chemical%20Sector.pdf>.

<http://www.dhs.gov/chemical-sector-training-and-resources#1> (Chemical Sector security resources and tools)

**5. Additional Recommended Reading:**

Mark Holt and Anthony Andrews, Cong. Research Service, RS 21131, Nuclear Power Plants: Vulnerability to Terrorist Attack(2007). <http://www.fas.org/sgp/crs/terror/RS21131.pdf>.

<http://www.infosecisland.com/blogview/4291-DHS-Cyber-Security-Resources-Catalog.html> (DHS Cyber Resources Catalog)

Hentea, Mariana. “Improving Security for SCADA Control Systems.” *Interdisciplinary Journal of Information, Knowledge, and Management* 3(March 2008).

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

Watts, David. “Security and Vulnerability in Electric Power Systems.” *35th North American Power Symposium, University of Missouri-Rolla in Rolla, Missouri* (October 20-21, 2003): 559-66.

<http://cip.management.dal.ca/publications/Security%20and%20Vulnerability%20in%20Electric%20Power%20Systems.pdf>.

**lesson 8 topic: sector profiles: transportation systems**

**1. Lesson Goals/Objectives**:

* Describe the sector’s operational profile, composite make-up, major critical infrastructure dependencies and interdependencies, and goals and objectives.
* Describe the sector’s risk profile and evaluate the sector’s approach to risk assessment, risk management, performance measurement, and incident management.
* Explain the PPD-8 core capabilities relevant to the sector and how they are delivered.
* Assess the sector’s regulatory profile (if applicable), as well as the strengths and limitations of regulation as a means to promote critical infrastructure security and resilience within the sector.
* Critique the various policies, plans, and programs in place to promote critical infrastructure security and resilience within the sector.

**2. Discussion Topics**:

* How is the sector organized to facilitate critical infrastructure security and resilience? Who are the key players? What are the key authorities that can be used to facilitate security and resilience within the sector?
* What are the sector’s goals and objectives relative to security and resilience?
* How do government and industry interact to promote critical infrastructure security and resilience within the sector? To support incident management activities? What formal coordination/collaboration structures/mechanisms are in place?
* How is information pertinent to critical infrastructure security and resilience shared and protected within the sector? What are the principal information sharing mechanisms utilized at the sector level? Are these effective? Do they need to be enhanced?
* How might PPD 21 and the Obama Administration’s Executive Order on Improving Critical Infrastructure Cybersecurity impact information sharing within the sectors studied in this lesson?
* Discuss the sector’s risk profile. What are the principal threats and hazards faced by the sector? What are the sector’s principal vulnerabilities or areas of concern from a security and resilience standpoint?
* What is the sector’s approach to risk assessment and risk management? How is performance measured and how is change effected based on areas where improvement is required?
* How does the sector approach the issue of cyber security? How do government and industry interact to jointly address cyber risk within the sector?
* What are the sector’s major dependencies and interdependencies from a security and resilience standpoint? How are dependencies/interdependencies issues identified and addressed within the sector?
* Which PPD-8 core capabilities are most relevant to the sector and how are they delivered? What work remains to be done in this area?
* Is the sector regulated from a security and resilience standpoint? If so, what are the major components of the regulatory framework? Is the existing regulatory framework effective, or does it need to be enhanced in some way?
* How is the sector postured to support emergent threat and incident management activities?
* Discuss the various policies, plans, and programs in place to promote critical infrastructure security and resilience within the sector. Are they effective? How could they be improved?

**3. In-class activity:** The class will be organized into 2 teams, with one team focusing on those aspects of the Transportation Systems Sector that fall under government regulation and the other focusing on those aspects of the Sector that operate according to a voluntary security construct. The instructor will facilitate a cross-team discussion of the strengths and weaknesses of each approach.

**4. Required Reading**:

Collins and Baggett, Chapters 8 and 9.

Lewis, Chapter 7, pp. 193-202; Chapter 9, pp. 249-263; and Chapter 10, pp. 291-303.

<https://www.hsdl.org/?view&did=736911>. (Transportation Systems Sector Specific Plan)

<http://training.fema.gov/EMIWeb/IS/IS860b/CIRC/transport1.htm> (Understanding the Transportation Systems Sector)

George Mason University, Center for Infrastructure Protection and Homeland Security. *The CIP Report* 11, no. 1 (July 2012). <http://cip.gmu.edu/wp-content/uploads/2014/01/July2012_SurfaceTransportation_FINAL.pdf>

Johnstone, Bill. “New Strategies to Protect America: Terrorism and Mass Transit after London and Madrid.” *Center for American Progress* (August 10, 2005).

<http://www.americanprogress.org/issues/security/news/2005/08/10/1592/new-strategies-to-protect-america-terrorism-and-mass-transit-after-london-and-madrid/>.

USCERT. *Roadmap to Secure Control Systems in the Transportation Sector* (2012). <https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/TransportationRoadmap20120831.pdf>

U.S. Gov’t Accountability Office, GAO-07-583T, Passenger and Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts(2007), <http://www.gao.gov/products/GAO-07-583T>.

U.S. Gov’t Accountability Office, GAO-09-243, 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>.

U.S. Gov’t Accountability Office, GAO-10-650T, Surface Transportation Security: TSA Has Taken Action to manage Risk, Improve Coordination, and Measure Performance, but Additional Actions Would Enhance Its Effort (2010).

<http://www.gao.gov/new.items/d10650t.pdf>.

U.S. Gov’t Accountability Office, GAO-13-20, Passenger Rail Security: Consistent Incident Reporting and Analysis Need to Achieve Program Objectives (2012). <http://www.gao.gov/assets/660/650995.pdf>

Blank Rome, *New Rail Security Rules in the U.S.* (December 2, 2008), <https://www.blankrome.com/index.cfm?contentID=31&itemID=1492>.

Paul Parfomak, Cong. Research Service, RL 33347, Pipeline Safety and Security: Federal Programs (2008).

<http://www.fas.org/sgp/crs/homesec/RL33347.pdf>.

**4. Additional Recommended Reading:**

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

Federal Transit Administration. *Transit Security Design Considerations*. Washington, DC: U.S. Department of Transportation, 2004.<http://www.tisp.org/index.cfm?cdid=10944&pid=10261>.

**lesson 9 topic: sector profiles: water and healthcare and public health**

**1. Lesson Goals/Objectives**:

* Describe the sector’s operational profile, composite make-up, major critical infrastructure dependencies and interdependencies, and goals and objectives.
* Describe the sector’s risk profile and evaluate the sector’s approach to risk assessment, risk management, performance measurement, and incident management.
* Explain the PPD-8 core capabilities relevant to the sector and how they are delivered.
* Assess the sector’s regulatory profile (if applicable), as well as the strengths and limitations of regulation as a means to promote critical infrastructure security and resilience within the sector.
* Critique the various policies, plans, and programs in place to promote critical infrastructure security and resilience within the sector.

**2. Discussion Topics**:

* How is the sector organized to facilitate critical infrastructure security and resilience? Who are the key players? What are the key authorities that can be used to facilitate security and resilience within the sector?
* What are the sector’s goals and objectives relative to security and resilience?
* How do government and industry interact to promote critical infrastructure security and resilience within the sector? To support incident management activities? What formal coordination/collaboration structures/mechanisms are in place?
* How is information pertinent to critical infrastructure security and resilience shared and protected within the sector? What are the principal information sharing mechanisms utilized at the sector level? Are these effective? Do they need to be enhanced?
* How might PPD 21 and the Obama Administration’s Executive Order on Improving Critical Infrastructure Cybersecurity impact information sharing within the sectors studied in this lesson?
* Discuss the sector’s risk profile. What are the principal threats and hazards faced by the sector? What are the sector’s principal vulnerabilities or areas of concern from a security and resilience standpoint?
* What is the sector’s approach to risk assessment and risk management? How is performance measured and how is change effected based on areas where improvement is required?
* How does the sector approach the issue of cyber security? How do government and industry interact to jointly address cyber risk within the sector?
* What are the sector’s major dependencies and interdependencies from a security and resilience standpoint? How are dependencies/interdependencies issues identified and addressed within the sector?
* Which PPD-8 core capabilities are most relevant to the sector and how are they delivered? What work remains to be done in this area?
* Is the sector regulated from a security and resilience standpoint? If so, what are the major components of the regulatory framework? Is the existing regulatory framework effective, or does it need to be enhanced in some way?
* How is a planning baseline established in sectors that are not subject to security regulations? What are the strengths and weaknesses of a purely voluntary approach to critical infrastructure security and resilience?
* How is the sector postured to support emergent threat and incident management activities?
* Discuss the various policies, plans, and programs in place to promote critical infrastructure security and resilience within the sector. Are they effective? How could they be improved?
* How would a pandemic outbreak impact the sectors discussed in this lesson? How do these two sectors impact other sectors in the context of a pandemic?

**3. In-class Activity**: For this lesson, the class will be broken down into 2 teams. Each team will be assigned readings corresponding to one of the two sectors studied in this lesson. Each team will be prepared to discuss their sector’s operational and risk profiles, the sector approach to risk assessment and management, sector information sharing mechanisms, etc. In turn, the instructor will facilitate a discussion of the differences and commonalities, as well as the strengths and weaknesses of the various approaches. The instructor will also facilitate a comparative discussion of regulatory regimes, where they exist, as well as PPD-8 capabilities delivery within the sectors.

**4. Required Reading**:

<https://www.hsdl.org/?view&did=736910>. (Water and Healthcare and Public Health)

Water Sector Coordinating Council,

<http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/water1.htm> (Understanding the Water Sector)

<http://water.epa.gov/infrastructure/watersecurity/mutualaid/index.cfm>

Water Environment Federation, *Water Sector Interdependencies*, (2011), <http://www.wef.org/uploadedFiles/Access_Water_Knowledge/Water_Security_and_Emergency_Response/Final_WEF_Summary_WSI.pdf>

Critical Infrastructure Partnership Advisory Council Water Sector Strategic Planning Working Group, *Roadmap to a Secure and Resilient Water Sector*, (2009), <http://www.nawc.org/uploads/documents-and-publications/documents/document_5582326a-7a35-4f67-923b-279c642b5129.pdf>

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

Congressional Research Service, *Safeguarding the Nation’s Drinking Water: EPA and Congressional Actions,* (September 30, 2010)*,* <http://www.fas.org/sgp/crs/misc/RL31294.pdf>

George Mason University, Center for Infrastructure Protection and Homeland Security. *The CIP Report* 11, no. 3 (September 2012). <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/TheCIPReport_September2012_Water.pdf>

George Mason University, Center for Infrastructure Protection and Homeland Security. *The CIP Report* 7, no. 11 (May 2009). <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_May2009_WaterSector1.pdf>

*Roadmap to Secure Control Systems in the Water Sector*, (March 2008),

<http://www.energetics.com/resourcecenter/products/roadmaps/samples/Documents/Water_Security_Roadmap.pdf>.

<http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/publicHealth1.htm> (Understanding the Healthcare and Public Health Sector)

<http://www.phe.gov/preparedness/planning/cip/Pages/default.aspx> (U.S. Department of Health and Human Services)

<http://www.phe.gov/Preparedness/planning/cip/Pages/initiatives.aspx> (U.S. Department of Health and Human Services)

<http://www.phe.gov/Preparedness/planning/cip/Documents/2010cikrannualreport.pdf> (Sector Annual Report)

<http://www.nasemso.org/Membership/MemberBenefits/documents/HSIN-HPHflyer.pdf> (Information Sharing)

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>

George Mason University, Center for Infrastructure Protection and Homeland Security. *The CIP Report* 8, no. 3 (September 2009). <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_September2009_BiosafetyandBiosecurity1.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: sector profiles: food and agriculture**

**1. Lesson Goals/Objectives**:

* Describe the sector’s operational profile, composite make-up, major critical infrastructure dependencies and interdependencies, and goals and objectives.
* Describe the sector’s risk profile and evaluate the sector’s approach to risk assessment, risk management, performance measurement, and incident management.
* Explain the PPD-8 core capabilities relevant to the sector and how they are delivered.
* Assess the sector’s regulatory profile (if applicable), as well as the strengths and limitations of regulation as a means to promote critical infrastructure security and resilience within the sector.
* Critique the various policies, plans, and programs in place to promote critical infrastructure security and resilience within the sector.

**2. Discussion Topics**:

* How is the sector organized to facilitate critical infrastructure security and resilience? Who are the key players? What are the key authorities that can be used to facilitate security and resilience within the sector?
* What are the sector’s goals and objectives relative to security and resilience?
* How do government and industry interact to promote critical infrastructure security and resilience within the sector? To support incident management activities? What formal coordination/collaboration structures/mechanisms are in place?
* How is information pertinent to critical infrastructure security and resilience shared and protected within the sector? What are the principal information sharing mechanisms utilized at the sector level? Are these effective? Do they need to be enhanced?
* How might PPD 21 and the Obama Administration’s Executive Order on Improving Critical Infrastructure Cybersecurity impact information sharing within the sectors studied in this lesson?
* Discuss the sector’s risk profile. What are the principal threats and hazards faced by the sector? What are the sector’s principal vulnerabilities or areas of concern from a security and resilience standpoint?
* What is the sector’s approach to risk assessment and risk management? How is performance measured and how is change effected based on areas where improvement is required?
* How does the sector approach the issue of cyber security? How do government and industry interact to jointly address cyber risk within the sector?
* What are the sector’s major dependencies and interdependencies from a security and resilience standpoint? How are dependencies/interdependencies issues identified and addressed within the sector?
* Which PPD-8 core capabilities are most relevant to the sector and how are they delivered? What work remains to be done in this area?
* Is the sector regulated from a security and resilience standpoint? If so, what are the major components of the regulatory framework? Is the existing regulatory framework effective, or does it need to be enhanced in some way?
* How is a planning baseline established in sectors that are not subject to security regulations? What are the strengths and weaknesses of a purely voluntary approach to critical infrastructure security and resilience?
* How is the sector postured to support emergent threat and incident management activities?
* Discuss the various policies, plans, and programs in place to promote critical infrastructure security and resilience within the sector. Are they effective? How could they be improved?

**3. In-class Activity**: For this lesson, the class will be broken down into 2 teams. Each team will be assigned readings corresponding to one of the two sectors studied in this lesson. Each team will be prepared to discuss their sector’s operational and risk profiles, the sector approach to risk assessment and management, sector information sharing mechanisms, etc. In turn, the instructor will facilitate a discussion of the differences and commonalities, as well as the strengths and weaknesses of the various approaches. The instructor will also facilitate a comparative discussion of regulatory regimes, where they exist, as well as PPD-8 capabilities delivery within the sectors.

**4. Required Reading**:

<http://www.dhs.gov/critical-infrastructure-sectors> (Food and Agriculture)

<http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/agFood1.htm> (Understanding the Food and Agriculture Sectors)

<http://www.fsis.usda.gov/food_defense_%26_emergency_response/index.asp> (FDA Food Defense Website)

<http://www.fernlab.org/fooddefense.cfm> (Food Emergency Response Network Website)

<http://www.nasda.org/cms/7196/7349.aspx> (United States and China Outline Progress on Agreement on Food and Feed Safety)

“Agro-Defense: Responding to Threats Against America's Agriculture and Food System” Statement of Ted Elkin, Director, Office of Food Defense, Center for Food Safety and Applied Nutrition, Food and Drug Administration ,Department of Health and Human Services. Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate (September 13, 2011), <http://www.fda.gov/NewsEvents/Testimony/ucm271077.htm>

<http://foodsafety.news21.com/2011/safety/prevention/fsma-provisions> (National Agriculture and Food Defense Strategy)

<http://foodshield.typepad.com/announcements_docs/What_is_FoodSHIELD_June07.pdf> (FOODshield)

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>

<http://www.fema.gov/pdf/emergency/nrf/nrf_FoodAgricultureIncidentAnnex.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 11 topic: sector profiles: critical manufacturing and defense industrial base**

**1. Lesson Goals/Objectives**:

* Describe the sector’s operational profile, composite make-up, major critical infrastructure dependencies and interdependencies, and goals and objectives.
* Describe the sector’s risk profile and evaluate the sector’s approach to risk assessment, risk management, performance measurement, and incident management.
* Explain the PPD-8 core capabilities relevant to the sector and how they are delivered.
* Assess the sector’s regulatory profile (if applicable), as well as the strengths and limitations of regulation as a means to promote critical infrastructure security and resilience within the sector.
* Critique the various policies, plans, and programs in place to promote critical infrastructure security and resilience within the sector.

**2. Discussion Topics**:

* How is the sector organized to facilitate critical infrastructure security and resilience? Who are the key players? What are the key authorities that can be used to facilitate security and resilience within the sector?
* What are the sector’s goals and objectives relative to security and resilience?
* How do government and industry interact to promote critical infrastructure security and resilience within the sector? To support incident management activities? What formal coordination/collaboration structures/mechanisms are in place?
* How is information pertinent to critical infrastructure security and resilience shared and protected within the sector? What are the principal information sharing mechanisms utilized at the sector level? Are these effective? Do they need to be enhanced?
* How might PPD 21 and the Obama Administration’s Executive Order on Improving Critical Infrastructure Cybersecurity impact information sharing within the sectors studied in this lesson?
* Discuss the sector’s risk profile. What are the principal threats and hazards faced by the sector? What are the sector’s principal vulnerabilities or areas of concern from a security and resilience standpoint?
* What is the sector’s approach to risk assessment and risk management? How is performance measured and how is change effected based on areas where improvement is required?
* How does the sector approach the issue of cyber security? How do government and industry interact to jointly address cyber risk within the sector?
* What are the sector’s major dependencies and interdependencies from a security and resilience standpoint? How are dependencies/interdependencies issues identified and addressed within the sector?
* Which PPD-8 core capabilities are most relevant to the sector and how are they delivered? What work remains to be done in this area?
* Is the sector regulated from a security and resilience standpoint? If so, what are the major components of the regulatory framework? Is the existing regulatory framework effective, or does it need to be enhanced in some way?
* How is a planning baseline established in sectors that are not subject to security regulations? What are the strengths and weaknesses of a purely voluntary approach to critical infrastructure security and resilience?
* How is the sector postured to support emergent threat and incident management activities?
* Discuss the various policies, plans, and programs in place to promote critical infrastructure security and resilience within the sector. Are they effective? How could they be improved?

**3. In-class Activity**: For this lesson, the class will be broken down into 2 teams. Each team will be assigned readings corresponding to one of the two sectors studied in this lesson. Each team will be prepared to discuss their sector’s operational and risk profiles, the sector approach to risk assessment and management, sector information sharing mechanisms, etc. In turn, the instructor will facilitate a discussion of the differences and commonalities, as well as the strengths and weaknesses of the various approaches. The instructor will also facilitate a comparative discussion of regulatory regimes, where they exist, as well as PPD-8 capabilities delivery within the sectors.

**4. Required Reading**:

http://www.dhs.gov/critical-infrastructure-sectors (Critical Manufacturing and Defense Industrial Base)

<http://training.fema.gov/EMIWeb/IS/is860a/CIRC/critManuf1.htm> (Understanding the Critical Manufacturing Sector)

http://cip.gmu.edu/wp-content/uploads/2014/01/March2012\_CriticalManufacturing\_FINAL.pdf

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>

<http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/defense1.htm> (Understanding the Defense Industrial Base Sector)

<http://policy.defense.gov/OUSDPOffices/ASDforHomelandDefenseAmericasSecurityAffa/DefenseCriticalInfrastructureProgram/Partnering.aspx>

George Mason University, Center for Infrastructure Protection and Homeland Security. *The CIP Report* 9, no. 11 (May 2011). http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS\_TheCIPReport\_May2011\_DIB.pdf

Government Accountability Office, *Defense Critical Infrastructure: DoD’s Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets*, (2008), <http://www.gao.gov/new.items/d08373r.pdf>

Government Accountability Office, *Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electric Power Risks and Vulnerabilities to DoD Critical Assets*, (October 2009), <http://transition.fcc.gov/pshs/docs/clearinghouse/GAO_Defense_Critical_Infrastructure_102009.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 12 topic: cross-sector dependencies and interdependencies**

**1. Lesson Goals/Objectives**:

* Explain and provide examples of how dependencies, interdependencies, and supply chain issues impact critical infrastructure risk assessment and management.
* Discuss how the various critical infrastructure sectors approach the issue of dependencies/interdependencies, including cross-sector cyber security risks, and supply chain risk.
* Explain and provide examples of how dependencies/interdependencies and supply chain considerations are factored in the critical infrastructure security and resilience planning process, as well as gaps in this process.
* Explain how dependencies/interdependencies complicate incident response decision making and infrastructure restoration operations.
* Critique the major elements of the National Strategy for Supply Chain Security.

**2. Discussion Topics**:

* What does the NIPP have to say regarding critical infrastructure dependencies and interdependencies across sectors?
* How do dependencies, interdependencies, and supply chain issues relate to critical infrastructure risk? How are infrastructure dependencies/interdependencies typically considered in the risk assessment process?
* How can dependencies/interdependencies best be accounted for in the planning process within and across the critical sectors and at various levels of government?
* How do infrastructure dependencies/interdependencies complicate incident response decision making and infrastructure restoration operations?
* How do regulatory regimes deal with “outside-the-fence” security concerns as well as critical dependency/interdependency issues?
* How have critical infrastructure dependency/interdependency issues manifested themselves in recent real world incidents? How do they impact incident recovery?
* What types of risk are represented by the “geographic clustering” of critical infrastructure? How has this risk manifested itself in recent natural disaster situations?
* What types of risk are represented by cross-sector cyber connections? How can they best be addressed?
* How do international supply chains complicate traditional approaches to risk assessment and management?
* What are the major goals and guiding principles that underpin the National Strategy for Global Supply Chain Security? How does this strategy address critical infrastructure dependencies/ interdependencies issues? How does the Strategy propose to reduce critical offshore infrastructure vulnerabilities beyond the control of the U.S.?
* How can a global strategy addressing supply chain security 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 Exercise**: Learners will be organized into teams and be prepared to discuss critical infrastructure dependencies/interdependencies in the context of recent real world incidents such as the Japanese Tsunami, Super Storm Sandy, Northeast Power Blackout, etc.). The focus of the discussion will be on impacts and risk response activities, along with key lessons learned. The instructor will make team assignments at the end of class on Lesson 11. This assignment will require additional Internet research. No formal presentation will be required.

**4. Required Reading**:

Steven Rinaldi, James Peerenboom, and Terrence Kelly, *Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies*, (2004), <http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf>.

George Mason University, Center for Infrastructure Protection and Homeland Security. *The CIP Report* 9, no. 2 (August 2011). <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_August2011_Interdependencies.pdf>

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

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

USCERT, *Cross Sector Roadmap for Cyber-Security of Control Systems*, (September 30, 2011), <http://www.us-cert.gov/control_systems/pdf/Cross-Sector_Roadmap_9-30.pdf>

Xavier Guiho, Patrick Lagadec, and Erwan Lagadec,

*Non-conventional Crises and Critical Infrastructure: Katrina*, (2006), <http://www.patricklagadec.net/fr/pdf/EDF-Katrina-Report-31.pdf>.

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/>

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>

1. **Additional Recommended Reading:**

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>

Rae Zimmerman, *Understanding the Implications of Critical Infrastructure Interdependencies for Water*, (2009), <http://research.create.usc.edu/cgi/viewcontent.cgi?article=1083&context=published_papers&sei-redir=1&referer=http%3A%2F%2Fwww.google.com%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3Dcritical%2520infrastructure%2520interdependencies%26source%3Dweb%26cd%3D7%26ved%3D0CGoQFjAG%26url%3Dhttp%253A%252F%252Fresearch.create.usc.edu%252Fcgi%252Fviewcontent.cgi%253Farticle%253D1083%2526context%253Dpublished_papers%26ei%3DKIfLUKXOKeee2wWZuYGoCA%26usg%3DAFQjCNFKpSLFck0WBFMa4h5myky4nKYdmw%26bvm%3Dbv.1355325884%2Cd.b2I#search=%22critical%20infrastructure%20interdependencies%22>

**lesson 13 topic: critical infrastructure interdependencies exercise**

**\*\*special activity:**

**incident management point paper due via email at the beginning of class**.

Today’s class involves an interactive, discussion-based Tabletop Exercise (TTX) driven by a scenario involving a Category 3 hurricane striking the Gulf Coast of the United States. The scenario will consist of three modules (Pre-Season/Pre-Landfall, Immediate Post-Landfall Response, and Post-Incident Recovery) in chronological sequence. The scenario and discussion questions by phase are included in Attachment 1. The TTX will focus on roles, responsibilities, and interaction between government and industry critical infrastructure partners in the context of an emergent threat as well as an incident in progress. Discussion will focus on critical infrastructure security and resilience-related communication and information sharing, coordination, integration of capabilities, and problem identification and resolution.

**1. Lesson Goals/Objectives**:

* Assess the various critical infrastructure sector dependencies /interdependencies and their related impacts brought to light by the exercise scenario.
* Describe the various roles and responsibilities of interdependent government and private sector critical infrastructure stakeholders in the context of an emergent threat as well as an incident in progress.
* Describe how the various critical infrastructure sector dependencies/interdependencies played out in the exercise scenario impact sector-specific situation assessments, stakeholder decision making, and response options.
* Discuss the nexus between the various mission area frameworks under PPD-8 (Response, Recovery, and Mitigation) as they relate to critical infrastructure impacts and stakeholder interaction as influenced by the exercise scenario.
* Identify and critique government-private sector information sharing and risk management products, processes, and systems relevant to critical infrastructure dependencies/interdependencies in the context of incident management operations.

**2. Discussion Topics**:

* What are the most significant infrastructure and infrastructure stakeholder dependencies/interdependencies brought to light by the scenario?
* How do infrastructure dependency/interdependency issues exacerbate the physical and psychological impacts of the incident? Could these impacts have been known in advance? If so, how should/would they influence planning and preparatory activities across the PPD-8 mission area frameworks?
* How do infrastructure dependencies/interdependencies impact incident response and recovery options and actions?
* What are the roles and responsibilities of the various government and industry sector partners under the NIPP, as well as under the various PPD-8 mission area frameworks (Response, Recovery and Mitigation)? How do these relate to critical infrastructure dependency/interdependency issues?
* What are the key government and private sector incident management nodes according to the NIPP and the NRF? How do these nodes communicate and coordinate with one another in the context of an emergent threat or incident in progress?
* How is information pertinent to critical infrastructure dependencies/ interdependencies shared between the various government and private sector nodes of the NIPPPartnership Framework in the context of the exercise scenario? Is the process effective, and how does it affect real-time decision making?
* What actions do the sectors take in response to the various phases of the incident lifecycle? What are the near, medium, and long-term ramifications of actions taken by one sector on the other sectors?
* How is situational awareness maintained among the various NIPP partners during incident response and recovery? Does this include a focus on critical infrastructure dependencies/interdependencies?
* How do critical infrastructure dependencies/interdependencies affect recovery planning and decision making?

**3. Required Reading**:

**General:**

Review highlights of the PPD-8 mission area frameworks (Response, Recovery and Mitigation).

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>

**Hurricane Scenario (See Attachment 1)**

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

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>.

**4. Additional Recommended Reading:**

*National Incident Management System*, (2008), <http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf>.

*Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 93-288)* <http://www.fema.gov/about/stafact.shtm>.

**lesson 14 topic: collaborative sector specific plan (ssp) critique presentations**

**\*\*special activity: collaborative written ssp critique is due via e-mail at the beginning of class on lesson 15**.

**1. Lesson Goals/Objectives**:

* Provide the highlights and foster classroom discussion on the SSP critiques and alternative approaches developed by the individual learner teams.

**2. Discussion Topics**:

* Learner Team presentations.

**3. Required Reading**:

* As required for written critique development and presentation.

**lesson 15 topic: collaborative SSP critique presentations and course wrap-up**

**\*\*special activity: collaborative ssp critique is due via e-mail by the beginning of class today**.

**1. Lesson Goals/Objectives**:

* Provide the highlights and foster classroom discussion on the SSP critiques and alternative approaches developed by the individual learner teams.

**2. Discussion Topics**:

* Team presentations.
* Course wrap-up and final thoughts.
* Course critique.

**3. Required Reading**:

* As required for written critique and presentation.

**ATTACHMENT 1**

**INFRASTRUCTURE INTERDEPENDENCIES EXERCISE**

**HURRICANE SCENARIO**

**module 1A: pre-season**

1. **Scenario Build**

* The Atlantic hurricane season extends from June 1st through November 30th each year, with the peak hurricane threat extending from mid-August to late October. Annually, an average of 11 tropical storms develops in the Atlantic Ocean, Caribbean Sea, or Gulf of Mexico, six of which typically become hurricanes. This year’s hurricane season is expected to be particularly active. The National Hurricane Center (NHC) is predicting 12-18 named storms, 6-8 hurricanes, and 2-3 major hurricanes for this upcoming hurricane season. In comparison, the NHC’s historical averages from 1966-2009 are 11.3 named storms, 6.2 hurricanes, and 2.3 major hurricanes.

* While hurricanes and their accompanying storm surges pose the greatest threat to life and property, tropical depressions and tropical storms can also be devastating. In addition, storm surge can account for a large number of casualties and personal property damage. Flooding resulting from storm surge or heavy rains and severe weather, such as tornadoes, can also cause loss of life and extensive damage.
* Preparation for, response to, recovery from, and mitigation against hurricanes require a coordinated response involving Federal, State, local, tribal, and territorial governments, the private sector, and nongovernmental organizations. This in-classroom exercise will be focused on the coordinated actions of the critical infrastructure community in preparation for and response to a generalized hurricane threat as well as a specific catastrophic storm.

1. **Discussion Questions:**

* How do the various critical infrastructure security and resilience government and private sector partners prepare jointly and coordinate with each other prior to the onset of hurricane season each year? What form does this coordination take? How does the agency/organization that you represent fit into this scheme?
* How does the National Mitigation Framework relate to pre-season hurricane preparedness within the infrastructure security and resilience community?
* Is your organization/entity a participant in locally-based NIMS structures?
* What types of analytical products, storm forecasts, best practices information, etc., are available to help guide critical infrastructure security and resilience partner hurricane preparedness and planning activities? How is this information communicated within the NIPP framework?
* Does infrastructure interdependencies analysis figure prominently in pre-season preparedness activities? What are the principal sources of such analysis?
* What types of assistance can the National Infrastructure Simulation and Analysis Center provide State and local agencies and the private sector prior to the onset of hurricane season? How is this assistance accessed?
* What are the most significant concerns of the agency/organization that you represent at this stage of hurricane season?

**module 1B: pre-landfall (h-hour)**

1. **Scenario Build**

* At the end of August, a tropical disturbance formed off the coast of Africa. On September 1st, the tropical disturbance was designated as Tropical Storm Heidi, located west of the Cape Verde Islands. During the next few days, Heidi continued to strengthen and was officially designated a hurricane on September 2nd. By the early morning hours of September 4th, Heidi was upgraded to a major hurricane with sustained winds of 115mph based on aircraft reports and satellite imagery. Heidi passed near the Turks and Caicos Islands as a Category 3 hurricane on September 7th, with sustained winds of more than 120mph and entered the Gulf of Mexico on September 9th with little change in strength. The governors of Texas and Louisiana and big city mayors across the region plan to announce mandatory evacuations of citizens. Both State governors declare major emergencies and request Federal assistance. Initial Federal emergency equipment and supply caches are moved to forward staging areas outside the projected hurricane impact zone.

1. **Discussion Questions:**

* What actions does the organization/entity that you represent take at the 48 hours prior to landfall decision point? At 24 hours? At 12 hours?
* What are the principal concerns of the agency/organization that you represent at this stage? What are your information sharing and public-private sector coordination priorities?
* How do the various critical infrastructure security and resilience government and private sector partners coordinate with each other and maintain a common situational awareness prior to hurricane landfall? What form does this coordination take? How does the agency/organization that you represent fit into this scheme?
* What types of analytical products, storm forecasts, cascading impacts projections, best practices information, etc., are available to help guide critical infrastructure security and resilience partner actions at this stage? How is this information communicated within the NIPP framework?
* What types of assistance can the National Infrastructure Simulation and Analysis Center provide State and local agencies and the private sector prior and during this stage? (storm surge, wind damage, population displacement, specific sector-level impacts)
* What is the role of DHS at this stage? FEMA? State and local officials with critical infrastructure security and resilience responsibilities? Corporate emergency management officials?
* What key nodes of the NRF Critical Infrastructure Support Annex are activated at this point, and how do they interact with one another?
* What government policies and public messaging processes come into effect during this stage that may impact critical infrastructure owner/operators? (evacuation decisions, continuity of operations site activations, contra-flow transportation plans, MOUs with private sector entities, senior official public proclamations, etc.)
* What are the priorities of private sector entities within the projected path of the hurricane at this stage?

**module 2: landfall (h-hour + 24 hours)**

**1. Scenario Build**

* From September 9th through the 12th, Hurricane Heidi moved along a Northwest path in the Gulf of Mexico, threatening Southwest Louisiana and the Northern Texas Coast. There was much uncertainty as Heidi turned slowly north and then northeast over the next two days before finally making landfall in Southeastern Louisiana west of Grand Isle, LA, as a Category 4 storm during the early morning hours of September 14th.
* Widespread storm surge flooding occurred in Southeast Louisiana, with Federal protection levees overtopping in the metro New Orleans area, producing pockets of significant flooding in low lying areas along the Mississippi River. In addition, Heidi produced 8-10 inches of rainfall which aggravated the storm surge flooding and brought many of the major rivers north of Lake Pontchartrain into flood stage. Although Heidi weakened upon moving inland, strong winds and torrential rains make movement impossible even in areas that were not inundated by flood waters.
* Presidential disaster declarations are made for the impacted counties in TX and LA. Federal incident coordination structures and field offices are activated.
* Over 2.5 million people are displaced from the region running from Northeast Texas to New Orleans. Additionally, the following major infrastructure damages/disruptions are noted:
* Over 4M customers are without power in the region, to include numerous major hospitals and special needs facilities.
* Numerous major transformer towers are down in the SW Louisiana region.
* Major rail, mass transit, and highway networks are shut down and/or damaged.
* The I-10 bridge across Lake Pontchartrain has been dismembered in several places; other secondary and tertiary bridges are down throughout the region.
* Two major nuclear power plants in the region have suffered minor damages, but have been placed in shut down mode.
* Over a dozen major oil and natural gas pipelines are inoperative, with extent of damages unknown.
* More than one hundred Gulf oil platforms have been evacuated; several are now “free-floating.”
* Six major oil refineries in the region have been extensively damaged and will require long repair times.
* Cellular communications have been significantly degraded throughout the region; cell towers are down across the area.
* Dozens of major chemical plants and hazmat facilities are under 4-8 feet of water; numerous chlorine rail tankers are overturned on site throughout the area.
* The Mississippi River channel is blocked by floating debris and sunken vessels in numerous locations south of New Orleans and is temporarily closed to commercial traffic; major petroleum and agricultural import/export operations have been suspended.
* Gasoline is in short supply across the region; first responder operations have priority.
* Minor civil disorder and looting activities are reported in several cities and towns in the impacted area.

**2. Discussion Questions:**

* What are the principal concerns of the agency/organization that you represent at this stage? What are your information sharing requirements at this stage? How are you getting the information you need?
* How do the various critical infrastructure security and resilience government and private sector partners coordinate with each other and maintain a common situational awareness following hurricane landfall? What form does this coordination take? How does the agency/organization that you represent fit into this scheme?
* What types of analytical products, imagery, damage assessment, and cascading impacts analysis products/services are available to help guide critical infrastructure security and resilience partner actions at this stage? How is this information communicated within the NIPP framework?
* What is the role of DHS at this stage? FEMA? State and local officials with critical infrastructure security and resilience responsibilities? Other Federal agencies?
* What key nodes of the NRF Critical Infrastructure Support Annex are activated at this point, and how do they interact with one another?
* What government policies and public messaging processes come into effect during this stage that may impact critical infrastructure owner/operators? (evacuation decisions, continuity of operations site activations, contra-flow transportation plans, MOUs with private sector entities, senior official public proclamations, etc.)
* What are the priorities of private sector entities within the damage footprint of the hurricane at this stage? How are cascading impacts to infrastructure determined and acted upon? How do these cascading impacts affect infrastructure restoration operations?
* How are private sector requests for assistance communicated to and considered for action by State and Federal governments post-landfall?
* How are private sector facility security concerns addressed post-landfall? Damage assessments? Civil disorder and looting?
* How are critical infrastructure restoration priorities determined by government and industry at this point? How do infrastructure dependencies/interdependencies factor into this calculus?
* How do State and local officials deal with the issue of private sector restoration reentry and access? How does the Federal government weigh in on this issue?

**module 3: post-landfall to recovery (48 hours to 1 month from landfall)**

**1. Scenario Build**

* By September 15th, Heidi had weakened to a tropical storm and was located in eastern Mississippi, moving generally N-NE. Extensive rainfall and winds of 10-20 mph are noted along the path of the storm. By the 17th, Heidi has been downgraded to a tropical depression moving northward into the Ohio Valley and into Canada.
* Federal, State, and local officials are dealing with more than a million shelter inhabitants and otherwise displaced individuals. Property damage to residences and businesses across the hurricane impact zone has been extensive.
* Dozens of important critical infrastructure facilities are under 4-8 feet of standing water. Suspected hazmat releases into the ground and area waterways are prevalent throughout the area.
* Long-term impacts to the regional transportation network and power grid are extensive, particularly with regard to the major Interstate highway corridors and mass transit systems. The I-10 bridges will be down for at least 90 days.
* Over 2.5M customers remain without power for weeks into the event, with major transformer outage issues complicating restoration. Up to half a million customers may be without power for up to 60-90 days.
* Loss of pipeline capacity is causing major gas price hikes all along the Gulf Coast and Eastern Seaboard. Oil production in the Gulf area will take several months to be restored; regaining full production capacity remains doubtful.
* Most communications in the area have been restored within the first week of the event.
* Local water and waste water treatment facilities are inoperative across the region, exacerbating infrastructure restoration/recovery operations.

**2. Discussion Questions:**

* What are the principal concerns of the agency/organization that you represent at this stage? What are your information sharing requirements at this stage? How are you getting the information you need?
* How do the government and private sector organize to support long-term restoration and recovery operations? How do things “get turned back on” and in what sequence?
* What the major concerns at the sector level during this stage?
* How does the National Recovery Framework address critical infrastructure restoration, recovery, and rebuilding issues? How are critical infrastructure equities represented within the organizational structure for recovery as detailed in the National Recovery Framework?
* How are key decisions made and priorities established between government and industry during this stage (i.e. to rebuild vice relocate, etc.)? How are these communicated?
* How are key infrastructure dependency/interdependency issues identified and acted upon during the recovery process? How do these issues impact the recovery process?
* What is the role of DHS at this stage? FEMA? State and local officials with critical infrastructure security and resilience responsibilities? Other Federal agencies?
* What government policies and public messaging processes come into effect during this stage that may impact critical infrastructure owner and operators?
* How are private sector requests for assistance communicated to and considered for action by State and Federal governments in this stage?
* How are major lessons from this event applied to the next cycle of preparedness? How are new policies developed and implemented?
* What are the major takeaways that you have from this exercise?
* How would a different region of the country react to this scenario (i.e. Washington, D.C., NYC, etc.)?