**Certificate Program in Critical Infrastructure Security and Resilience**

**Course Number: XXXX**

**Advanced Topics in Critical Infrastructure Security and Resilience**

**University of XXXXXX Fall/Spring Semester 20XX**

**NAME OF SCHOOL:**

**DEPARTMENT:**

**PROFESSOR:** Telephone Number: Office Location: Office Hours:

Email: Website:

**COURSE DESCRIPTION/OVERVIEW:**

As discussed in the fundamentals course of this certificate program, the 21st century risk environment is a complex mix of manmade and naturally occurring threats and hazards including: terrorism, hurricanes, earthquakes, floods, power outages, environmental mishaps, industrial accidents, pandemic influenza, and cyber intrusions. Within this risk environment, our critical infrastructure are inherently interdependent—domestically and internationally—and vulnerable both within and across sectors due to the nature of their physical attributes, operational environments, international supply chains, and logical interconnections. Hence, the critical infrastructure mission area requires a focused national strategy and supporting plans and operational structures appropriately balancing resilience—a traditional American strength—with risk-informed prevention, protection, and preparedness activities that allow us to manage the most serious risks we face. Developing and putting this strategy and supporting plans and programs into practice, in turn, require an unprecedented partnership between the government and private sectors at all levels.

Federal, State, and local agencies and regional entities have a varied mix of authorities and capabilities, as well as unique concerns arising from the functional and geographical dependencies and interdependencies that characterize the concerned infrastructure within their jurisdictions and geographic boundaries. As in the case of the individual critical infrastructure sectors, these unique authorities, capacities, and concerns result in very different approaches and needs relative to the protection and resilience of critical infrastructure such as electric power transmission systems, pipelines, transportation grids, etc., that cross jurisdictional boundaries. The thread that pulls these disparate elements together is the process used to create strategies and plans that set the stage for success in both a steady state risk environment as well as during the response to emergent threats and incidents affecting critical infrastructures.

This course is a 15-lesson graduate-level seminar providing an advanced focus on critical infrastructure security and resilience policy, strategy, planning, and incident management operations in an all-hazards context. In terms of the audience, this course assumes a base level of learner knowledge and practical experience in the critical infrastructure security and resilience field. As such, it is targeted toward mid-career government and private sector professionals and members of the policy and academic communities with roles and responsibilities related to critical infrastructure security and resilience strategy development, planning, training, program management, and incident management operations. It is also targeted toward learners who have completed all prerequisite courses in the critical infrastructure certificate program series.

This course builds upon the knowledge attained in the introductory course and allows learners to apply this fundamental knowledge to “hands-on” critical infrastructure security and resilience case studies, in-class exercises, and scenario simulations. These “hands-on” exercises will reinforce knowledge and critical thinking skills taught in the certificate courses and ensure that learners fully recognize the “whole of community” nature of critical infrastructure security and resilience. It begins with an in-depth review of the strategic context presented by the 21st century risk environment, various critical infrastructure security and resilience policy and planning frameworks, and operational landscape across sectors and governmental jurisdictions, vertically and horizontally. It then examines the constituent elements of critical infrastructure security and resilience strategy development, planning, program management, and incident management, including the following: government-private partnership networks; information-sharing regimes; risk analysis and prioritization; risk mitigation; performance metrics; and incident management coordinating structures.

Working within the overall framework comprised by these elemental building blocks, the course next addresses the fundamentals of comprehensive critical infrastructure security and resilience strategic planning at the Federal, State, local, tribal, and territorial levels of government, as well as at the sector and corporate levels within industry.

The course concludes with an interactive module focused on the complexities of critical infrastructure security and resilience emergent threat response and incident management operations from an all-hazards perspective.

This course is designed to promote an advanced understanding of the various applications of critical infrastructure security and resilience strategies, plans, and incident management structures and coordinating processes across the Nation’s critical infrastructure sectors. It is also intended to promote advanced subject-matter understanding, critical issue analysis, and insight into senior leader risk assessment, decision-making, and planning processes. The course features a comprehensive practical examination of critical infrastructure stakeholder interaction and key subject-matter areas through a collaborative planning project, in-class exercises, interactive tabletop exercises, and an oral presentation.

**CREDITS CONFERRED:** 3

**PREREQUISITES:**

• Course Number XXXX: Foundations of Critical Infrastructure Security and

Resilience

• Course Number XXXX: Partnering and Information Sharing for Critical

Infrastructure Security and Resilience

• Course Number XXXX: Assessing and Managing Risk to Critical Infrastructure

Systems

• Course Number XXXX: Critical Infrastructure Security, Resilience, and

Cybersecurity

**COURSE GOALS/OBJECTIVES (AS MAPPED AGAINST U.S. DEPARTMENT OF HOMELAND SECURITY (DHS) CORE COMPETENCIES):**

This course is designed to enable learners to:

**1. Promote an advanced understanding of critical infrastructure security and resilience as a core homeland security policy area:**

• Course introduction and overview; and framing principles and concepts

• Review of the historical evolution of critical infrastructure security and resilience as a national policy area; and overarching policy approaches and implications for critical infrastructure security and resilience stakeholder community

• Review of Congressional engagement in the critical infrastructure policy area post- September 11, 2001, post-Katrina, and post-Sandy

• Re-examination of the September 11, 2001 attacks, Hurricane Katrina, Gulf oil disaster, Hurricane Sandy, and international cyber intrusions as strategic focusing events

**2. Promote an advanced understanding of critical infrastructure security and resilience-focused strategy and planning frameworks:**

• Quadrennial Homeland Security Review Report

• National Infrastructure Protection Plan and supporting Sector-Specific Plans

• DHS Guide to Critical Infrastructure Security at the State, local, tribal, territorial, and regional level

• The Infrastructure Security Partnership Regional Resilience Handbook

• Corporate security, emergency response, and business continuity plans

**3. Promote an advanced understanding of the 21st century risk environment in the context of the critical infrastructure security and resilience mission area:**

• Threats: terrorism, cyber attacks, natural disasters and naturally occurring phenomena, industrial accidents and technological failures, and other emergencies

• Vulnerabilities (facility, node, and system level)

• Consequences (public health and safety, economic loss/disruption, continuity of government and essential services, iconic loss, etc.)

• Dependencies/interdependencies.

• Informing executive and managerial decision-making related to critical infrastructure security and resilience plans and programs

**4. Expand familiarity with the authorities, roles, responsibilities, and capacities of key government and private sector stakeholders with critical infrastructure security and resilience responsibilities:**

• Federal, State, local, tribal, territorial, and private sector

• International

• Touch points and flash points

• Regulations, incentives, and other motivations

**5. Develop an advanced understanding of the building blocks of critical infrastructure security and resilience strategy development, planning, and incident management operations:**

• **Critical infrastructure security and resilience partnership frameworks, information sharing processes/systems, and coordination/collaboration structures:**

o Federal, State, local, tribal, territorial, and private sector collaboration, coordination, and communication

o International partner collaboration, coordination, and communication

o Critical infrastructure data collection, warehousing, and protection

o All-hazards information sharing

o Challenges and opportunities

• **Critical infrastructure security and resilience risk analysis, risk mitigation, and performance measurement:**

o Physical security

o Cybersecurity

o Insider Threats (including personnel security)

o Resilience

o Systems dependencies/interdependencies

o Regional risk frameworks

o Sector considerations

• **Critical infrastructure sector-level approaches:**

o Agriculture and Food o Chemical

o Commercial Facilities

o Communications

o Critical Manufacturing

o Dams

o Defense Industrial Base

o Emergency Services

o Energy

o Financial Services

o Government Facilities

o Information Technology

o Nuclear Reactors, Materials, and Waste

o Healthcare and Public Health

o Transportation Systems

o Water and Wastewater Systems

**6. Evaluate critical infrastructure security and resilience strategy development, planning, and program management in a dynamic risk and future operating environment:**

• Developing corporate-level, sector-specific, jurisdictionally-based, or regionally-focused critical infrastructure security and resilience goals, objectives, risk mitigation approaches/plans, and measures of performance

• Designing and applying continuous feedback mechanisms to measure critical infrastructure security and resilience program performance

• Designing and implementing critical infrastructure security and resilience awareness, education, and training plans and programs

• Achieving critical infrastructure security and resilience in a resource constrained environment

• Planning for the future risk and critical infrastructure operational environments

**7. Apply the national critical infrastructure security and resilience incident management framework through selected case studies and in-class exercises:**

• National Incident Management System

• National Response Framework and Critical Infrastructure Support Annex/Cyber Incident Annex

• National Cyber Incident Response Plan

• September 11, 2001 Attacks

• Northeast Power Blackout 2003

• Madrid/London Transit Bombings (2004 and 2005)

• Hurricane Katrina (2005)

• California Wildfires

• Mumbai Attack (2008)

• Gulf of Mexico Oil Spill (2010)

• Joplin, Missouri Tornado (2011)

• Hurricane Sandy (2012)

• Boston Marathon Bombing (2013)

• Cyber Threats and Incidents

**DELIVERY METHOD/COURSE REQUIREMENTS:**

Course delivery will be through mini-lectures, structured collaborative projects and 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 (government products that are responsive or attempt to fulfill the requirements of authoritative documents), and external reviews (U.S. Government Accountability Office (GAO), Congressional Research Service (CRS), etc.). Learners are expected to familiarize themselves with the assigned topic and readings before class and should be prepared to discuss and debate them critically as well as analyze them for biases from multiple perspectives. The instructor will facilitate the discussion by asking different levels of questioning (factual, analytical, and application of the material) to evaluate the depth of the learner’s comprehension of the content.

**GRADING:**

Classroom Participation 20% Collaborative Planning Project 35% Oral Presentation 15% Incident Management Exercises 1&2 30% (including player roles/responsibilities point papers)

Total 100%

**ORAL/WRITTEN REQUIREMENTS:**

**1. Collaborative Planning Project/Oral Presentation (50%):**

Learners will work collaboratively in 2-3 person teams to develop a critical infrastructure security and resilience strategy, plan, or program targeted at the corporate (enterprise level), sector, jurisdictional (Federal, State, local, tribal, and territorial government), regional, or international level. For template purposes, learners should refer to the structure and content used in the NIPP, various NIPP Sector-Specific Plans, DHS’ *Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal and Territorial Level,* the Infrastructure Security Partnership’s *Regional Disaster Resilience Guide,* recognized corporate-level business continuity plan, international strategy, or published standard.

Each team will present the highlights of its strategy, plan, or program to the class during Lessons 13-14 using one of the formats discussed above. This presentation should involve all team members and be no more than 45 minutes in length. **The completed written project deliverable is to be submitted no later than the day of Lesson 15 for all project teams.**

Prior approval of the focus area selected for the collaborative planning project is required. **Teams should submit a one-page written description of their proposed focus area in class or via email for approval no later than the beginning of class in Lesson 4.**

**(Note: Submission deadline may be extended with instructor approval.)**

**2. Incident Management Exercises (30%):**

Learners will participate in two role-based, interactive tabletop exercises. The first will simulate a complex, physical-cyber terrorist attack on critical infrastructures and population centers within the United States. The outline for this exercise is provided in **Attachment 1**. The second tabletop exercise will focus on critical infrastructure preparations for and response to a Category 4 hurricane striking the Gulf Coast of the United States. The outline for this exercise is provided in **Attachment 2**. 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., governor, mayor, secretary of homeland security, municipal police chief, state homeland security advisor/emergency manager, corporate security director, etc.). The exercises will include an emerging threat phase, operational response phase, and post-incident recovery phase.

In preparation for each exercise, each learner will develop a short 2-3 page paper in bulleted talking point format delineating his/her assigned role-based responsibilities during each phase of exercise play. **This paper will be submitted at the beginning of class on the day of each scheduled classroom exercise.** Individual roles for each exercise will be assigned by the instructor during class in **Lesson 4**.

**3. Expectations for Participation (20%):**

Participation includes coming to class prepared, engaging in class discussions, particpating as a full partner in group activities, and actively role playing during the critical infrastructure security and resilience incident management exercises.

**INCORPORATION OF FEEDBACK**:

The course instructor will offer multiple opportunities for learners to provide constructive feedback over the period of the course. These feedback channels may take the form of group sessions or one-on-one sessions with the instructor. Learners will be afforded the opportunity to complete in-class evaluations at the end of Lesson 6, following the first of the two scheduled critical infrastructure incident management exercises, 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 planning project, group oral presentation, and incident management point papers. Ongoing dialogue with the instructor regarding project development, oral presentation preparation, and incident management 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.

Ted G. Lewis, ed., *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Wiley-Interscience, 2006).

Pamela A. Collins and Ryan Keith Baggett, *Homeland Security and Critical Infrastructure*

*Protection* (Praeger Security International, 2009).

**GRADING SCALE (SCHOOL POLICY DEPENDENT):**

**COURSE OUTLINE**

**LESSON 1 TOPIC: COURSE OVERVIEW AND 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, and feedback processes.

• Describe the evolution of critical infrastructure as a national policy focus area.

• Discuss the various statutes and Presidential policy documents governing the application of critical infrastructure security and resilience in the United States, including their application to strategy development and planning.

• Explain how critical infrastructure security and resilience policies and plans have evolved as a function of the all-hazards risk environment.

• Explain the general critical infrastructure operational landscape across the sectors and the United States regionally.

**2. Discussion Topics:**

• How would you characterize the major shifts in U.S. critical infrastructure policy over time? Are we where we need to be?

• How have the definition of “critical infrastructure” and the scope of the critical infrastructure security and resilience sector-focused construct have changed over time?

* What are the principal variations across sectors regarding critical infrastructure?

• Why does critical infrastructure security and resilience represent such a challenge within and across governmental jurisdictions and sectors?

• What are the general principles we typically associate with critical infrastructure security and resilience in the U.S. context?

• 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 operations?

• How has the Nation’s approach to critical infrastructure security and resilience preparedness and planning changed over time and with regard to certain threats/hazards?

• What are the differences between, and strengths and weaknesses of, the various Presidential policies focused on critical infrastructure security and resilience over the last 15 years?

• How does the U.S. Congress view the critical infrastructure security and resilience mission area? Does legislation clarify or complicate the critical infrastructure security and resilience mission space?

• Where should the next Administration/Congress take the critical infrastructure security and resilience mission area?

**3. In-class Exercise:** Learners will be asked to work in small teams during the second half of class to develop a “model framework” for critical infrastructure security and resilience based on the last 15 years of domestic policy evolution and practical application. Each team will provide an informal presentation of their model program and engage in debate with the other teams.

**4. Required Reading**:

Lewis, *Critical Infrastructure Protection in Homeland Security*, chaps. 1-2.

Collins and Baggett, *Homeland Security and Critical Infrastructure*

*Protection*, chaps. 1-3.

Robert T. Marsh, “Critical Foundations: Protecting America’s Infrastructures,” *George C. Marshall Institute*, November 12, 1997, [http://www.marshall.org/article.php?id=65.](http://www.marshall.org/article.php?id=65)

Presidential Decision Directive 63: Critical Infrastructure Protection, May 22, 1998, [http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.](http://www.fas.org/irp/offdocs/pdd/pdd-63.htm)

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, February 12, 2013, <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

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

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

Congressional Research Service*,* Critical Infrastructures: Background, Policy, and

Implementation, February 21, 2014,  [http://www.fas.org/sgp/crs/homesec/RL30153.pdf.](http://assets.opencrs.com/rpts/RL30153_20100607.pdf)

U.S. Department of Homeland Security*,* Quadrennial Homeland Security Review, June 18, 2014,  [http://www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.pdf.](http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf)

**5. Additional Recommended Reading:**

The White House, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February2003, [http://www.dhs.gov/xlibrary/assets/Physical\_Strategy.pdf.](http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf)

The White House Homeland Security Council, National Strategy for Homeland Security, October 2007, <http://www.hsdl.org/?view&did=479633>.

**LESSON 2 TOPIC: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE STRATEGY AND PLANNING FRAMEWORKS**

**1. Lesson Goals/Objectives**:

•

• Recognize and evaluate major efforts to develop and implement critical infrastructure security and resilience and business continuity strategies and initiatives at the Federal, State, local, tribal, and territorial level, as well as across the private sector.

• Describe the concepts of “prevention,” “protection,” and “resilience,” as they relate to the critical infrastructure security and resilience mission area.

• Analyze the concept of “community resilience” as it relates to critical infrastructure security and resilience planning.

**2. Discussion Topics**:

• What are the major planning frameworks that guide preparedness and planning and critical infrastructure security and resilience program development within and across government and industry?

• How do these frameworks intersect/inter-relate with one another? Are there gaps? Inconsistencies? Major differences?

• 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?

• What is the concept of “resilience” and how does it apply in the context of critical infrastructure security and resilience planning?

• What are the general principles 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 various approaches to operationalize resilience at a regional and sub-regional level?

• 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?

**3. Required Reading**:

Brandon J. Hardenbrook, “The Need for a Policy Framework to Develop Disaster Resilient Regions,” *Journal of Homeland Security and Emergency Management* 2(3) art. 2 (2005), <http://www.degruyter.com/view/j/jhsem.2005.2.3/jhsem.2005.2.3.1133/jhsem.2005.2.3.1133.xml?format=INT>.

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

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

The Infrastructure Security Partnership, *Regional Disaster Resilience Guide*,

(2011),  [http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.tisp.org%2Ftisp%2Ffile%2FTemplate\_TISP%2520Layout\_v29(2).pdf&ei=U3eoU8-QMYOpyATB0oGwBg&usg=AFQjCNFely9sgVUrn2BKaaCwq-hG-UvaBA&sig2=VsXAA5s1Y8MUbtLM3G\_o0Q&bvm=bv.69411363,d.aWw (](http://www.tisp.org/index.cfm?cdid=11493&pid=10261)general review only).

National Infrastructure Advisory Council, *Critical Infrastructure Resilience Final Report and Recommendations*, September 2009, [http://www.dhs.gov/xlibrary/assets/niac/niac\_critical\_infrastructure\_resilience.pdf.](http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf)

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

U.S. Government Accountability Office, *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*, March 2010, [http://www.gao.gov/new.items/d10296.pdf.](http://www.gao.gov/new.items/d10296.pdf)

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 9(8), (February 2011), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_February2011_Resilience.pdf>.

Ready Business, *Business Emergency Plan: Business Continuity and Disaster Preparedness Plan*, [http://www.ready.gov/business/\_downloads/sampleplan.pdf.](http://www.ready.gov/business/_downloads/sampleplan.pdf)

**4. Recommended Additional Reading:**

Fire Department of the City of New York, *Terrorism and Disaster Preparedness Strategy*, 2007, [http://www.nyc.gov/html/fdny/html/publications/tdps/tdps.shtml.](http://www.nyc.gov/html/fdny/html/publications/tdps/tdps.shtml)

U.S. Government Accountability Office, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, October 2007, [http://www.gao.gov/new.items/d08212t.pdf.](http://www.gao.gov/new.items/d08212t.pdf)

Yacov Y. Haimes, “On the Complex Definition of Risk: A Systems-Based Approach,”

*Risk Analysis*, 29(12), (2009), 1647-1654,

<http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2009.01310.x/full>.

Yacov Y. Haimes, “On the Definition of Resilience in Systems,” *Risk Analysis*, 29(4), (2009), 498-501, <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2009.01216.x/pdf>.

**LESSON 3 TOPIC: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE PLANNING FOUNDATIONS: AUTHORITIES, ROLES AND RESPONSIBILITIES OF FEDERAL, STATE, LOCAL, AND PRIVATE SECTOR PARTNERS**

**1. Lesson Goals/Objectives**:

• Describe the authorities, roles, and responsibilities of government (Federal, State, local, tribal, territorial, and international) and the private sector regarding critical infrastructure security and resilience.

• Compare and contrast regulated and voluntary critical infrastructure security and resilience regimes across the critical sectors.

• Describe the roles that nongovernmental organizations, the scientific/technology community, and academia play in critical infrastructure security and resilience.

• Evaluate the principal political, organizational, legal, and resource challenges that those responsible for critical infrastructure security and resilience face in executing those responsibilities.

**2. Discussion Topics**:

• Who is responsible for critical infrastructure security and resilience nationally, regionally, locally, and across the critical infrastructure sectors? How is critical infrastructure security and resilience planning structured/conducted at each jurisdictional level? Between the public and private sectors horizontally?

• What are the key authorities, roles, responsibilities, and capacities of the following with respect to critical infrastructure security and resilience:

* + Federal, State, local, tribal, and territorial governments; industry; academia; Research and Development (R&D) entities; and nongovernmental organizations?

• How are each of the above players advantaged/disadvantaged regarding their individual critical infrastructure security and resilience planning roles and responsibilities?

• How do the various government and private entities with critical infrastructure security and resilience responsibilities at different levels interact and collaborate with one another?

• What are the roles and responsibilities of the DHS Protective Security Advisors (PSAs) and Sector Specialists within the NIPP Partnership Framework?

• 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?

• How does the fractured structure of responsibility and accountability play out vis-a-vis the principal threats we face in this mission area?

• Does our national policy and planning framework effectively and efficiently enable critical infrastructure security and resilience planning and program implementation at the regional level? State level? Local level? Corporate level?

• How are high impact, low frequency threats addressed in the NIPP framework? Across sectors? Within industry?

**3. In-class Exercise:** The class will be divided into three teams, each representing a major critical infrastructure community of interest: Federal departments and agencies, State and local agencies, and private industry. Each team will develop a list of their specific roles and responsibilities as well as principal concerns within the critical infrastructure and resilience mission area. The instructor will then lead a guided discussion across the three teams, drawing each into the discussion of key policy and planning issues.

**4. Required Reading**:

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, February 12, 2013, <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

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

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

Sue Eckert, “Protecting Critical Infrastructure: The Role of the Private Sector”

(2005), [http://www.ridgway.pitt.edu/LinkClick.aspx?fileticket=Bezaq7AdjxA%3D&tabi](http://www.ridgway.pitt.edu/LinkClick.aspx?fileticket=Bezaq7AdjxA%3D&tabid=233) [d=233.](http://www.ridgway.pitt.edu/LinkClick.aspx?fileticket=Bezaq7AdjxA%3D&tabid=233)

Ken Schnepf, “SLTTGCC Coordinates State and Local Infrastructure Security Efforts,” *Plant Services* (2007), [http://www.plantservices.com/articles/2007/198.html.](http://www.plantservices.com/articles/2007/198.html)

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

**LESSON 4 TOPIC: ASSESSING CRITICAL INFRASTRUCTURE RISK IN AN INTERDEPENDENT WORLD**

**\*\*SPECIAL ACTIVITY: INCIDENT MANAGEMENT EXERCISE ROLES ASSIGNED BY INSTRUCTOR/PROFESSOR**.

**\*\*SPECIAL ACTIVITY: COLLABORATIVE PLANNING PROJECT FOCUS AREA DESCRIPTION DUE TO INSTRUCTOR/PROFESSOR**.

**1. Lesson Goals/Objectives**:

• Analyze the major elements of risk in the context of critical infrastructure security and resilience planning: threats, vulnerabilities, and consequences.

• Critique the DHS strategic risk assessment process and how other government and private sector critical infrastructure stakeholders view and evaluate risk.

• Identify and discuss the complexities regarding critical infrastructure dependencies and interdependencies as they relate to risk.

• Explain the relationship between risk and critical infrastructure risk management strategies, plans, and resource investment across government and the private sector.

• Assess the challenges associated with critical infrastructure 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?

• How has the nature of the risks to our critical infrastructure evolved over time?

• What are the principal challenges we face in ensuring the security and resilience of our critical infrastructure in light of these risks?

• How does the NIPP address the subject of risk? How are risks prioritized within the NIPP framework? Other government frameworks? Business continuity planning frameworks?

• How do the human, physical, and cyber dimensions of critical infrastructure security and resilience relate to the concept of risk?

• How does the Federal government assess risk and communicate the results of the risk assessment process to other critical infrastructure stakeholders? Do these other players have a role to play in government risk assessment processes and programs?

• How does risk management relate to strategic decisions, 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?

• Is there room for subjectivity in the risk analysis process?

• How does the issue of critical infrastructure dependencies/interdependencies complicate the risk assessment process? How do we measure the dependencies factor? How do we factor interdependencies into the planning process?

• Can we ever get to a totally risk-based critical infrastructure security and resilience construct?

• Should we base the allocation of critical infrastructure-related grant funding on the notion of risk? Is the system working?

• Do the uncertainties surrounding risk quantification hinder our intuitive understanding of risk?

• What are the advantages/disadvantages of the various approaches to risk as practiced within the NIPP Partnership Framework?

**3. Required Reading**:

Collins and Baggett, *Homeland Security and Critical Infrastructure Protection*, chaps. 5, 13, and 15.

Lewis, *Critical Infrastructure Protection in Homeland Security*, chap. 4, pp. 71-73; chap. 5, pp. 107-110; and chap. 13.

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

Congressional Research Service, *Critical Infrastructures: What Makes Infrastructure Critical?*, August 30, 2002,

[http://www.libertysecurity.org/IMG/pdf/CRS\_Report\_-\_What\_makes\_an\_Infrastructure\_](http://www.libertysecurity.org/IMG/pdf/CRS_Report_-_What_makes_an_Infrastructure_Critical_-_30.08.2002.pdf)

[Critical\_-\_30.08.2002.pdf.](http://www.libertysecurity.org/IMG/pdf/CRS_Report_-_What_makes_an_Infrastructure_Critical_-_30.08.2002.pdf)

Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, *Complex Networks* (2001), [http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.](http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf)

Congressional Research Service*, Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options*, September 18, 2008, [http://assets.opencrs.com/rpts/RL33206\_20080912.pdf.](http://assets.opencrs.com/rpts/RL33206_20080912.pdf)

George Mason University, Critical Infrastructure Protection Program, *Critical Infrastructure Protection: Elements of Risk*, chap. 3, <http://cip.gmu.edu/archive/archive/RiskMonograph_1207_r.pdf>.

Robert A. Miller and Irving Lachow, “Strategic Fragility: Infrastructure Protection and National Security in the Information Age,” Defense Horizons No. 59 (2008), [http://www.carlisle.army.mil/DIME/documents/Miller%20and%20Lachow%20St](http://www.carlisle.army.mil/DIME/documents/Miller%20and%20Lachow%20Strategic%20Fragility.pdf) [rategic%20Fragility.pdf.](http://www.carlisle.army.mil/DIME/documents/Miller%20and%20Lachow%20Strategic%20Fragility.pdf)

Brian A. Jackson and David R. Frelinger, “Emerging Threats and Security Planning: How Should We Decide What Hypothetical Threats to Worry About,” *RAND Corporation* (2009), <http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP256.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 10(5), (November 2011), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_November2011_RiskManagement.pdf>.

**4. Recommended Additional Reading:**

Xavier Guiho, Patrick Lagadec, and Erwan Lagadec,

“Non-Conventional Crises and Critical Infrastructure: Katrina,” *EDF*

(2006), [http://www.patricklagadec.net/fr/pdf/EDF-Katrina-Report-31.pdf.](http://www.patricklagadec.net/fr/pdf/EDF-Katrina-Report-31.pdf)

U.S. Government Accountability Office, *Risk Management: Strengthening the Use of Risk*

*Management Principles in Homeland Security*, (June 25, 2008), [http://www.gao.gov/products/GAO-08-904T.](http://www.gao.gov/products/GAO-08-904T)

Congressional Research Service, *Banking and Financial Institution Continuity: Pandemic*

*Flu, Terrorism, and Other Challenges*, (May 4, 2009),

[http://www.fas.org/sgp/crs/misc/RL31873.pdf.](http://www.fas.org/sgp/crs/misc/RL31873.pdf)

The National Academies Press, *Review of the Department of Homeland Security’s*

*Approach to Risk Analysis*, (2010), [http://www.nap.edu/catalog.php?record\_id=12972,](http://www.nap.edu/catalog.php?record_id=12972)

Congressional Research Service, *International Terrorism and Transnational*

*Crime: Security Threats, U.S. Policy, and Considerations for Congress* (January 5,

2010), <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Ffpc.state.gov%2Fdocuments%2Forganization%2F134960.pdf&ei=HYWoU9WJMaOF8AHK1YGgDA&usg=AFQjCNFKa-QlsLADvJdIU-7hZlhUi_PeVA&sig2=lQfGwEKSvLNtWOA-yAn41Q&bvm=bv.69411363,d.b2U>.

Congressional Research Service, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy* (January 25, 2011), [http://www.fas.org/sgp/crs/terror/R41070.pdf.](http://www.fas.org/sgp/crs/terror/R41070.pdf)

**LESSON 5 TOPIC: ENABLING SECURITY, MANAGING RISK, AND MEASURING PERFORMANCE THROUGH REGULATION**

**\*\*SPECIAL ACTIVITY: INSTRUCTOR WILL ASSIGN INDIVIDUAL NIPP SECTOR SPECIFIC PLAN (SSP) READINGS FOR LEARNER DISCUSSION ON LESSON 6.**

**1. Lesson Goals/Objectives**:

• Evaluate the different ways in which risk is assessed and managed and how performance is evaluated in those sectors in which security is regulated by a government entity.

• Describe the relationship between a regulator and regulated party in the context of critical infrastructure security and resilience.

• Explain how the government-private regulatory relationship affects the planning and performance measurement processes.

**2. Discussion Topics**:

• What are the different approaches to security regulation across the sectors? How does each address the major areas of risk assessment, management, and performance measurement?

• How do the regulators and regulated parties relate to one another in these different approaches/models?

• What are the strengths and weaknesses of a regulatory approach to critical infrastructure security and resilience?

• How does the private sector view the issue of security regulation with the critical infrastructure mission area? Of the various models employed within the critical sectors, which regulatory approach is most favored by the private sector?

• Is there one or more model of regulation that stands out as more effective than the others? If so, why?

• How do regulatory regimes deal with “outside-the-fence” security concerns as well as critical dependency/interdependency issues?

• Is regulation working to produce a measurable increase in security in those sectors in which regulation is operative?

• How does regulation impact the planning and performance measurement processes?

• Why have other industrialized countries avoided a regulatory regime for some sectors that the United States regulates?

• Should cybersecurity be regulated within and across the critical sectors? Is cybersecurity regulation effective within the electricity sub sector?

**3. Required Reading**:

Collins and Baggett, *Homeland Security and Critical Infrastructure*

*Protection*, chaps. 6, 7, and 9.

*Maritime Transportation Security Act of* *2002*, Pub. L. No. 107-295 (2002) <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.gpo.gov%2Ffdsys%2Fpkg%2FPLAW-107publ295%2Fpdf%2FPLAW-107publ295.pdf&ei=Q4eoU_09yJOoBo-4gLAG&usg=AFQjCNHmyM7VhZTDxF-K8ibpfFe5ngU6BA&sig2=oBTvY4spAZ-FZ2Sri9VsJw&bvm=bv.69411363,d.b2k>.

U.S. Department of Homeland Security, *Chemical Facility Antiterrorism Standards* (2007), [http://www.dhs.gov/files/laws/gc\_1166796969417.shtm.](http://www.dhs.gov/files/laws/gc_1166796969417.shtm)

Congressional Research Service, *Nuclear Power Plants: Vulnerability to Terrorist*

*Attack* (August 9, 2007), [http://www.fas.org/sgp/crs/terror/RS21131.pdf.](http://www.fas.org/sgp/crs/terror/RS21131.pdf)

Congressional Research Service, *Pipeline Safety and Security: Federal Programs* (February 29, 2008), [http://www.fas.org/sgp/crs/homesec/RL33347.pdf.](http://www.fas.org/sgp/crs/homesec/RL33347.pdf)

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

U.S. Government Accountability Office, *Freight Rail Security: Actions Have Been Taken to Enhance Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored* (April 2009), [http://www.gao.gov/new.items/d09243.pdf.](http://www.gao.gov/new.items/d09243.pdf)

**LESSON 6 TOPIC: ENABLING SECURITY, MANAGING RISK, AND MEASURING PERFORMANCE IN A VOLUNTARY PARADIGM**

**1. Lesson Goals/Objectives**:

• Evaluate how risks are assessed and managed and how performance is evaluated in those sectors in which security is not regulated by a government entity.

• Describe the relationship between the government at all levels and the private sector in a voluntary security construct.

**2. Discussion Topics**:

• What are the different approaches to voluntary security collaboration and coordination across the sectors? How does each address the major areas of risk assessment, management, and performance measurement?

• How is a planning baseline established in sectors that are not subject to security regulations?

• How does government at various levels relate to the private sector in these various sector level approaches/models?

• What are the strengths and weaknesses of a purely voluntary approach to critical infrastructure security and resilience? How is joint critical infrastructure -related planning accomplished in a voluntary model?

• Is there one model of voluntary security collaboration/coordination that stands out as more effective than the others? If so, why?

• How do voluntary security regimes deal with “outside-the-fence” security concerns as well as critical dependency/interdependency issues?

• 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?

• What are the pros and cons of the DHS PS-Prep program? What is (are) the next step(s) that this program needs to take to be successful?

**3. In-class exercise:** Learners will read and be prepared to informally discuss/critique one of the NIPP Sector Specific Plans (SSPs) in detail in class. Learners will be assigned a sector plan for the focus of this discussion by the instructor at the end of class on Lesson 5.

**4. Required Reading**:

Collins and Baggett, *Homeland Security and Critical Infrastructure*

*Protection*, chaps. 8 and 9.

Lewis, *Critical Infrastructure Protection in Homeland Security*, chap. 7, pp. 193-202; chap. 9, pp. 249-263; and chap. 10, pp. 291-303.

Peter R. Orszag, “Critical Infrastructure Protection and the Private Sector: The Crucial

Role of Incentives,” *Brookings* (September 4, 2003),

<http://www.brookings.edu/research/testimony/2003/09/04-homelandsecurity-orszag>.

U.S. Department of Transportation, *Transit Security Design Considerations*, November 2004, [http://www.tisp.org/index.cfm?cdid=10944&pid=10261.](http://www.tisp.org/index.cfm?cdid=10944&pid=10261)

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

“The Challenge of Protecting Critical Infrastructure,” *Wharton Risk Management and Decision Processes Center* (October 2005), [http://opim.wharton.upenn.edu/risk/downloads/05-11-EMK.pdf.](http://opim.wharton.upenn.edu/risk/downloads/05-11-EMK.pdf)

U.S. Government Accountability Office, *Passenger Rail Security: Federal Strategy and*

*Enhanced Coordination Needed to Prioritize and Guide Security Efforts*, March 7, 2007, [http://www.gao.gov/products/GAO-07-583T.](http://www.gao.gov/products/GAO-07-583T)

Bill Johnstone, “New Strategies to Protect America: Terrorism and Mass Transit after

London and Madrid,” *Center for American Progress* (August 10, 2005), <http://americanprogress.org/issues/security/news/2005/08/10/1592/new-strategies-to-protect-america-terrorism-and-mass-transit-after-london-and-madrid/>.

Congressional Research Service, *Terrorism and Security Issues Facing the Water Infrastructure Sector*, December 15, 2010, [http://www.fas.org/sgp/crs/terror/RL32189.pdf.](http://www.fas.org/sgp/crs/terror/RL32189.pdf)

U.S. Government Accountability Office, *Surface Transportation Security: TSA Has Taken Actions to Manage Risk, Improve Coordination, and Measure Performance, but Additional Actions Would Enhance Its Efforts*, April 21, 2010, [http://www.gao.gov/new.items/d10650t.pdf.](http://www.gao.gov/new.items/d10650t.pdf)

**LESSON 7 TOPIC: INFORMATION SECURITY AND INDUSTRIAL CONTROL SYSTEMS RISK PLANNING AND PERFORMANCE MEASUREMENT**

**1. Lesson Goals/Objectives**:

• Analyze the nature of the cyber threats and challenges that impact the critical infrastructure security and resilience mission area, including the authorities, capacities, and resources landscape of the cyber domain and how cyber risk is assessed and managed across sectors.

• Analyze the challenges represented by information technology and Supervisory Control and Data Acquisition (SCADA) systems vulnerabilities.

**2. Discussion Topics**:

• What are the principal threats and challenges of cybersecurity as they pertain to critical infrastructure security and resilience? Is this a “real and present danger?” Why or why not?

• How do various government documents address the problem? Are these effective approaches?

• How do cyber and industrial control systems (ICS) concerns relate to the critical infrastructure sectors?

• How are the sectors structured to deal with this evolving threat?

• How do the various critical infrastructure sectors address cyber and ICS vulnerabilities?

• Who “owns” the cyber problem? On the government side? On the private sector side? How does each party communicate and coordinate with the other to jointly address cyber risk and ICS vulnerabilities?

• How is cyber risk assessed and mitigated? How do we know when we are making a difference in this domain? How can risk reduction be measured?

• Is Federal regulation required to mitigate risk across all sectors subject to the cyber threat? If so, what would such a regime look like?

• How is the cyber dimension factored into critical infrastructure security and resilience-focused strategies and plans?

• How is planning in the cyber domain different from conventional domains?

**3. Required Reading**:

Collins and Baggett, *Homeland Security and Critical Infrastructure*

*Protection*, chap. 10.

Lewis, *Critical Infrastructure Protection in Homeland Security*, chap. 8, pp. 223-244 and chap. 14, pp. 429-440, 454-459.

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

National Institute of Standards and Technology, *Framework for Improving*

*Critical Infrastructure Cybersecurity*, February 12, 2014, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>

Jason Stamp, Phil Campbell, Jennifer DePoy, John Dillinger, and William Young,

“Sustainable Security for Infrastructure SCADA,” *Sandia National Laboratories*, 2003, [http://energy.sandia.gov/wp/wp-content/gallery/uploads/SustainableSecurity.pdf.](http://energy.sandia.gov/wp/wp-content/gallery/uploads/SustainableSecurity.pdf)

Keith Stouffer, Joe Falco, and Karen Kent, “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrialized Control Systems Security,” *National Institute of Standards and Technology*, September 2006, <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=https%3A%2F%2Fwww.dhs.gov%2Fsites%2Fdefault%2Ffiles%2Fpublications%2Fcsd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf&ei=rb-pU6fdOuTN8wGS7IGoCw&usg=AFQjCNHnjUgT2aPpeayzDkBUr5gv_eu5Xw&sig2=rRJtJaHcoFkcP91mZuCEaA&bvm=bv.69620078,d.b2U>.

Mariana Hentea, “Improving Security for SCADA Control Systems,” *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 2 (2008), [http://ijikm.org/Volume3/IJIKMv3p073-086Hentea361.pdf.](http://ijikm.org/Volume3/IJIKMv3p073-086Hentea361.pdf)

U.S. Government Accountability Office, *Critical Infrastructure Protection: DHS Needs to Better Address its Cybersecurity Responsibilities*, September 16, 2008, [http://www.gao.gov/products/GAO-08-1157T.](http://www.gao.gov/products/GAO-08-1157T)

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 7(8), (February 2009), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_February2009_SCADA.pdf>.

The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 29, 2009, [http://whitehouse.gov/assets/documents/Cyberspace\_Policy\_Review\_final.pdf.](http://whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)

U.S. Government Accountability Office, *Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats*, June 16, 2010, [http://www.gao.gov/new.items/d10834t.pdf.](http://www.gao.gov/new.items/d10834t.pdf)

**4. Additional Recommended Reading:**

“Roadmap to Secure Control Systems in the Water Sector,” *Water Sector Coordinating Council Cyber Security Working Group*, (March 2008),

<http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.awwa.org%2Fportals%2F0%2Ffiles%2Flegreg%2Fsecurity%2Fsecurityroadmap.pdf&ei=S8KpU-m6C6OF8AGcpYDoCQ&usg=AFQjCNH7q4SoKERYFiADf3CUAK_4nlwV3A&sig2=D60C-rTCfeBiFukKSB4btQ&bvm=bv.69620078,d.b2U>.

**LESSON 8 TOPIC: APPROACHES TO ORGANIZING AND PARTNERING FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE AND NETWORKING TO SHARE INFORMATION**

**\*\*SPECIAL ACTIVITY: INSTRUCTOR WILL ASSIGN TEAM INTERNATIONAL CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE STRATEGY/PLAN/PROGRAM READINGS FOR LEARNER DISCUSSIONS ON LESSON 9**.

**1. Lesson Goals/Objectives**:

• Identify and critique the methods, processes, and systems that the various critical infrastructure security and resilience partners use to share information with one another, including those associated with the NIPP Partnership Model.

• Describe the ongoing challenges and barriers to information sharing and collaboration that exist between the various levels of government and the private sector.

• Evaluate 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?

• What is the value added nature of 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 are smaller size firms represented within the various SCCs? Does this representation vary across the sectors?

• How are trade associations represented within the various SCCs? How do they relate to individual corporations represented on the SCCs?

• How do the various elements of the NIPP Partnership Model interact with one another? 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 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 NIPP partnership 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, to include 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? Are we successfully “connecting the dots” today?

• How does information sharing factor into critical infrastructure security and resilience strategy and planning efforts?

• What does resilience really mean? Are some sectors more resilient than others by nature or construct?

**3. Required Reading**:

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

ISAC Council, *A Policy Framework for the ISAC Community*, January 31, 2004, <http://www.isaccouncil.org/images/Policy_Framework_for_ISAC_Community_013104.pdf>.

The White House, *National Strategy for Information Sharing*, October 2007,

<http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.fas.org%2Fsgp%2Flibrary%2Finfoshare.pdf&ei=nMOpU-m1EZazyASYj4HIBw&usg=AFQjCNHIqrD67nafvDe8HbSxmyosEFP3gw&sig2=Wq6718TpnAYcLZurNOvSoA&bvm=bv.69620078,d.aWw>.

U.S. Government Accountability Office, *Homeland Security: Federal Efforts Are Helping to Address Some Challenges Faced by State and Local Fusion Centers*, April 17, 2008, [http://www.gao.gov/new.items/d08636t.pdf.](http://www.gao.gov/new.items/d08636t.pdf)

Robert Riegle Testimony before the Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *The Future of Fusion Centers: Potential Promise and Dangers*, April 1, 2009, [http://www.dhs.gov/ynews/testimony/testimony\_1238597287040.shtm.](http://www.dhs.gov/ynews/testimony/testimony_1238597287040.shtm)

U.S. Department of Homeland Security, *State and Major Urban Area Fusion Centers*, <http://www.dhs.gov/state-and-major-urban-area-fusion-centers>.

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

**4. Recommend Additional Reading**:

Congressional Research Service, *Sharing Law Enforcement and Intelligence Information: The Congressional Role*, February 13, 2007, [http://www.fas.org/sgp/crs/intel/RL33873.pdf.](http://www.fas.org/sgp/crs/intel/RL33873.pdf)

U.S. Department of Homeland Security, *Critical Infrastructure Resource Center: Critical Infrastructure Partnerships*, <http://training.fema.gov/EMIWeb/IS/IS860b/CIRC/CIKRpartnerships.htm>.

**LESSON 9 TOPIC: THE INTERNATIONAL DIMENSION OF CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE STRATEGY AND PLANNING**

**1. Lesson Goals/Objectives**:

• Explain the international dimensions of critical infrastructure security and resilience and cybersecurity planning as defined in the NIPP, focusing on physical and virtual supply chain dependencies/ interdependencies in a global economy.

• Analyze the various alternative approaches to critical infrastructure security and resilience and cybersecurity planning in use internationally, including voluntary and regulatory models.

• Evaluate the various structures and forums that are used to promote international critical infrastructure security and resilience and cybersecurity cooperation and collaboration.

**2. Discussion Topics**:

• What does the NIPP have to say regarding the international dimension of critical infrastructure security and resilience? Cybersecurity?

• Why do we need to press for critical infrastructure security and resilience and cybersecurity outside our own borders? How do physical and virtual supply chain considerations factor into this equation?

• Who should be our principal international critical infrastructure security and resilience and cybersecurity partners? Why?

• How do we achieve domestic critical infrastructure security and resilience and cybersecurity in the context of a global economy?

• What are the typical approaches to critical infrastructure security and resilience and cybersecurity used outside the United States? What are their strengths and weaknesses?

• What are some examples of countries that use a purely voluntary approach to critical infrastructure security and resilience and cybersecurity? A purely regulatory approach? A hybrid approach?

• Does a “model” critical infrastructure security and resilience or cybersecurity regulatory program or “best practice” exist abroad?

• Is there an appropriate structure(s) through which international critical infrastructure security and resilience and cybersecurity issues can be addressed?

• Is there a national, bi-national, or multi-national critical infrastructure security and resilience or cybersecurity program that stands out as a model or best practice?

• How can multi-lateral international critical infrastructure security and resilience and cybersecurity cooperation and collaboration be incentivized?

• What should constitute the major elements of a U.S. international critical infrastructure security and resilience and cybersecurity strategy? How would such a strategy best be implemented and through what mechanism?

**3. In-Class Exercise**: Learners will be divided into teams and will be asked to present an informal synopsis and critique of a non-U.S. critical infrastructure security strategy, plan, or program (i.e. United Kingdom, Australia, Canada, European Union, etc.). Individual team assignments will be made by the instructor at the end of Lesson 8. This assignment will require additional Internet research. No formal presentation will be required.

**4. Required Reading**:

Arjen Boin, Mark Rhinard, and Magnus Ekengren, “Institutionalizing Homeland Security Cooperation in Europe: Counter-Terrorism and Critical Infrastructure Protection Compared,” *International Studies Association* (March 26, 2008), <http://citation.allacademic.com//meta/p_mla_apa_research_citation/2/5/0/8/6/pages250863/p250863-1.php>.

NATO Parliamentary Assembly, *The Protection of Critical Infrastructures*, 2007,

<http://www.nato-pa.int/default.asp?SHORTCUT=1165>.

European Commission, *Protecting Europe from Large-Scale Cyber-Attacks and Disruptions*, 2009, <http://europa.eu/legislation_summaries/information_society/internet/si0010_en.htm>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 8(1), (July 2009), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_July2009_InternationalCIP1.pdf>.

U.S. Department of Homeland Security and Public Safety Canada, *Canada-United States Action Plan for Critical Infrastructure*, 2010, <http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 8(12), (June 2010), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_June2010_InternationalCIP.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 9(12), (June 2011), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_June2011_InternationalCIP.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 10(1), (July 2011), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_July2011_GlobalSupplyChain.pdf>.

The White House, *International Strategy for Cyberspace: Prosperity, Security, and*

*Openness in a Networked World*, May 2011, [http://www.whitehouse.gov/sites/default/files/rss\_viewer/international\_strategy\_fo](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf) [r\_cyberspace.pdf.](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf)

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* *on Critical Information Infrastructure Protection: Achievements and Next Steps: Towards Global Cyber-Security*, March 31, 2011, [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF) [PDF.](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF)

**5. Recommended Additional Reading:**

Elgin M. Brunner and Manuel Suter, “International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies,” *Center for Security Studies, ETH Zurich*, (2008-09), <http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf>.

European Commission, *Recommended Elements of Critical Infrastructure Protection for*

*Policy Makers in Europe (RECIPE): Good Practices Manual for CIP Policies*,

2011, <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.oiip.ac.at%2Ffileadmin%2FUnterlagen%2FDateien%2FPublikationen%2FFINAL_RECIPE_manual.pdf&ei=vcupU6-1MOq78gGf2YCIDg&usg=AFQjCNH2L2Su_I4OGOoZXTspWoycs1oTsA&sig2=5d6v6d2U-CKjYpBqqgIr7w&bvm=bv.69620078,d.b2U&cad=rja>.

“IFIP Working Group 11.10 on Critical Infrastructure Protection,” *IFIP*, [http://www.ifip1110.org/Conferences/.](http://www.ifip1110.org/Conferences/)

**LESSON 10 TOPIC: MANAGING INCIDENTS IN AN ALL-HAZARDS ENVIRONMENT**

**\*\*SPECIAL ACTIVITY**: **INCIDENT MANAGEMENT EXERCISE PREP**: Today’s class involves a comprehensive walk-through of the National Response Framework (NRF) and National Cyber Incident Response Plan (NCIRP) as they relate to critical infrastructure security and resilience incident management. The intent is to help prepare learners for the interactive discussion that will take place during the tabletop exercises (TTXs) that will be conducted in Lessons 11 and 12. These TTXs will highlight incident management roles, responsibilities, coordinating structures, and interaction between Federal, State, local, tribal, and territorial agencies; the private sector; and the general public in the context of an emergent threat as well as an incident in progress. Participant 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 roles and responsibilities of government and private sector entities in the context of an emergent threat as well as an incident in progress.

• Describe key critical infrastructure security and resilience incident management nodes, coordinating structures, and processes through which the various public and private sector stakeholders interact as discussed in the NRF and its CIKR Support Annex, and the NCIRP *—* prevention, protection, mitigation, response, and recovery.

• Assess government-private sector information sharing and intelligence networks in the context of incident management.

• Evaluate the processes and mechanisms used to build critical infrastructure situational awareness and facilitate government-private prevention, protection, mitigation, response, and recovery activities during incidents.

**2. Discussion Topics**:

• What are the roles and responsibilities of the various NIPP partners vis-à-vis national incident management in a complex physical-cyber incident?

• What are the key government and private sector incident management nodes and coordinating structures as detailed in the NIPP, NRF and NCIRP? How do they interact with one another?

• How are information and intelligence shared between the various government and private sector nodes of the NIPP Partnership Framework in an emergent threat scenario? Does the process work?

• What actions do the sectors take in response to a national level NTAS/NCAS alert or emergent threat? What are the near and long-term ramifications across the sectors?

• How is situational awareness maintained among the various NIPP partners during incident response, including on the cyber side?

• How are private sector requests for assistance assessed and addressed during incident response operations?

**3. Required Reading**:

U.S. Department of Homeland Security, *National Response Framework*,

May 2013,  [http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final\_national\_response\_framework\_20130501.pdf.](http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf)

National Infrastructure Advisory Council, *The Framework for Dealing with Disasters and*

*Related Interdependencies Working Group*, July 14, 2009, [http://www.dhs.gov/xlibrary/assets/niac/niac\_framework\_dealingwithdisasters\_sli](http://www.dhs.gov/xlibrary/assets/niac/niac_framework_dealingwithdisasters_slides.pdf) [des.pdf](http://www.dhs.gov/xlibrary/assets/niac/niac_framework_dealingwithdisasters_slides.pdf)

U.S. Department of Defense, U.S. Department of Homeland Security, and U.S. Department of Justice, *Cyber Incident Annex*, December 2004, [http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fwww.fema.gov%2Fmedia-library-data%2F20130726-1825-25045-8307%2Fcyber\_incident\_annex\_2004.pdf&ei=DtCpU96NDomjyATk0oHICA&usg=AFQjCNHzW4wqmvfcw-d7yuTs4JGWu6tbcg&sig2=q2aXuF1jPCW8U13jFBexVA&bvm=bv.—69620078,d.b2U&cad=rja](http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fwww.fema.gov%2Fmedia-library-data%2F20130726-1825-25045-8307%2Fcyber_incident_annex_2004.pdf&ei=DtCpU96NDomjyATk0oHICA&usg=AFQjCNHzW4wqmvfcw-d7yuTs4JGWu6tbcg&sig2=q2aXuF1jPCW8U13jFBexVA&bvm=bv.69620078,d.b2U&cad=rja).

U.S. Department of Homeland Security, *National Cyber Incident Response Plan (Interim Version)*, September 2010, [http://www.federalnewsradio.com/pdfs/NCIRP\_Interim\_Version\_September\_201](http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf)

[0.pdf.](http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf)

U.S. Department of Homeland Security, *United States Computer Emergency Readiness Team*, [http://www.us-cert.gov.](http://www.us-cert.gov/)

U.S. Department of Homeland Security, *Industrial Control Systems Cyber Emergency Response Teams*, <https://ics-cert.us-cert.gov/>.

**4. Additional Recommended Reading:**

U.S. Department of Homeland Security, *National Incident Management System*,

December 2008, [http://www.fema.gov/pdf/emergency/nims/NIMS\_core.pdf.](http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf)

Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 93-288 (2013)[http://www.fema.gov/about/stafact.shtm.](http://www.fema.gov/about/stafact.shtm)

**LESSON 11 TOPIC: CISR INCIDENT MANAGEMENT EXERCISE #1**

**\*\*SPECIAL ACTIVITY:**

**INCIDENT MANAGEMENT POINT PAPER (#1) DUE VIA EMAIL PRIOR TO CLASS**.

Today’s class involves an interactive, discussion-based table top exercise (TTX) driven by a complex, physical-cyber terrorism-based scenario — one of the most challenging hybrid threats currently facing the infrastructure security mission area. This scenario will consist of four modules (Pre-incident, Warning, Activation, and Extended Response) in chronological order and portrays a series of improvised explosive device (IED) attacks against critical infrastructure target sets and cyber systems across multiple sectors and regions of the United States. The TTX will address the roles, responsibilities, and interactions between Federal, State, local, territorial, and tribal government entities; the private sector; and the general public in the context of an emergent threat as well as a complex incident in progress. Learner discussion will focus on critical infrastructure security and resilience-related communication and information sharing, coordination, integration of capabilities, and problem identification and resolution. A complete outline of the exercise is located at **Attachment 1**.

**1. Lesson Goals/Objectives:**

**• Apply course themes in the context of a terrorism-based incident management TTX.**

**2. Discussion Topics:**

**• See Attachment 1.**

**3. Required Reading:**

**• See Lesson 10.**

**LESSON 12 TOPIC: CISR INCIDENT MANAGEMENT EXERCISE #2**

**\*\*SPECIAL ACTIVITY:**

**INCIDENT MANAGEMENT POINT PAPER (#2) DUE VIA EMAIL PRIOR TO CLASS**.

Today’s class involves an interactive, discussion-based TTX driven by a natural disaster scenario. This scenario will consist of four modules (Pre-season, Pre-landfall, Landfall, and Post-landfall) in chronological order and portrays a Category 4 hurricane making landfall along the Gulf Coast of the United States. The TTX will focus on roles, responsibilities, and interaction between Federal, State, local, territorial, and tribal government entities; the private sector; and the general public 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. A complete outline of the exercise is located at **Attachment 2**.

**1. Lesson Goals/Objectives:**

**• Apply course themes in the context of a natural disaster incident management TTX.**

**2. Discussion Topics:**

**• See Attachment 1.**

**3. Required Reading:**

**• See Lesson 10.**

**LESSON 13 TOPIC: COLLABORATIVE PLANNING PROJECT PRESENTATIONS**

**\*\*SPECIAL ACTIVITY: COLLABORATIVE PLANNING PROJECT WRITTEN DELIVERABLE IS DUE VIA E-MAIL ON LESSON 15**.

**1. Lesson Goals/Objectives**:

• Provide the highlights and foster classroom discussion on the critical infrastructure security and resilience strategy, plan, or program developed by the Planning Team.

**2. Discussion Topics**:

• Planning Team presentations.

**3. Required Reading**:

• As required for project development and presentation.

**LESSON 14 TOPIC: COLLABORATIVE PLANNING PRESENTATIONS**

**\*\*SPECIAL ACTIVITY: COLLABORATIVE PLANNING PROJECT DELIVERABLE IS DUE VIA E-MAIL ON LESSON 15**.

**1. Lesson Goals/Objectives**:

• Provide the highlights and foster classroom discussion on the critical infrastructure security and resilience strategy, plan, or program developed by the Planning Team.

**2. Discussion Topics**:

• Planning Team presentations.

**3. Required Reading**:

• As required for research paper and presentation.

**LESSON 15 TOPIC: COURSE WRAP-UP: PREPARING AND PLANNING FOR THE FUTURE CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE RISK ENVIRONMENT**

**\*\*SPECIAL ACTIVITY: COLLABORATIVE PLANNING PROJECT DELIVERABLE IS DUE VIA E-MAIL ON LESSON 15**.

**1. Lesson Goals/Objectives**:

• Discuss potential future critical infrastructure operational and risk environments and related challenges.

• Assess the strategic choices that may impact our approach to critical infrastructure security and resilience planning in the medium-long term future.

• Describe the types of planning efforts and investments that must begin to happen now to adequately prepare for the future world of critical infrastructure security and resilience.

• Analyze the Federal, State, local, tribal, territorial, and private sector critical infrastructure security and resilience requirements processes.

• Evaluate the importance of critical infrastructure security and resilience awareness, education, and training programs today and in the future.

**2. Discussion Topics**:

• What will the critical infrastructure security and resilience operational environment look like 10-20 years from now?

• How do we best plan for it given the constraints we face today?

• What are our options for dealing with the recapitalization of our aging infrastructure base?

• What will be the principal threats and challenges to critical infrastructure security and resilience and cybersecurity in this future world?

• What insights do we have on the nature of future critical infrastructure dependencies and interdependencies?

• Can the future world of critical infrastructure security and resilience and cybersecurity be simulated and “war-gamed” today?

• What actions should we be taking now to buy down future risk and position the next generation for success in this issue area? Will today’s priority focus areas set us up for success? Are we focused on the right issues moving forward?

• What are the metrics that will guide relevant critical infrastructure security and resilience and cybersecurity feedback processes in the future?

• How are critical infrastructure security and resilience-related requirements determined and resourced within government? Industry? Across sectors? Are these processes sufficient to get us ready for the future?

• How do we begin to address planning concerns that transcend the next budget cycle?

• How can we achieve truly integrated critical infrastructure security and resilience and cybersecurity planning in the future across sectors and jurisdictions?

• How can critical infrastructure security and resilience goals and objectives be harmonized within and across sectors, jurisdictions, and geographic regions?

• What are the core elements of an effective critical infrastructure security and resilience and cybersecurity awareness, education, and training program?

• What are the keys to an effective critical infrastructure security and resilience program management today and in the future?

• What is the critical infrastructure job market?

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

**4. Required Reading**:

Brian A. Jackson, “Marrying Prevention and Resiliency,” *RAND* (2008), <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCQQFjAA&url=http%3A%2F%2Fwww.rand.org%2Fcontent%2Fdam%2Frand%2Fpubs%2Foccasional_papers%2F2008%2FRAND_OP236.pdf&ei=pdSpU4vSN8ia8QHFtIF4&usg=AFQjCNEU5zBle8EQ1rPCHRN2Lu2YAk5rUA&sig2=crYEuoaY9TNGr29n8-VOBg&bvm=bv.69620078,d.b2U>.

American Society of Civil Engineering, *The Infrastructure Crisis*, Civil Engineering, January 2008, [http://www.tisp.org/index.cfm?cdid=11036&pid=10261.](http://www.tisp.org/index.cfm?cdid=11036&pid=10261)

Toffler Associates, *Guarding Our Future: Protecting our Nation’s Infrastructure*, 2008, <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.toffler.com%2Fassets%2F1%2F6%2FGuarding-Our-Future.pdf&ei=btWpU5rONs6NqAbt0YGYCw&usg=AFQjCNFt-5X0pfWxaz49qDynBkvmYeAl6w&sig2=OkiDCio1muBOeFTde2hiFg&bvm=bv.69620078,d.b2k>.

Toffler Associates, *Five Critical Threats to the Infrastructure of the Future: Leading Infrastructure Protection Experts Discuss Strategies for Protecting Your Enterprise*, 2008, <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB0QFjAA&url=http%3A%2F%2Fwww.somanco.com%2Fdocuments%2FFive%2520Critical%2520Infrastructure%2520Threats.pdf&ei=s9WpU8nxHeTN8wGS7IGoCw&usg=AFQjCNEtdy0akD_KBLq17oV5ufyDtkWn-g&sig2=AHjPWAwQ5D1awm3IUvMmag&bvm=bv.69620078,d.b2k>.

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

National Research Council of the National Academies, *Sustainable Critical Infrastructure Systems: A Framework for Meeting 21st Century Imperatives*, 2009, [http://www.nap.edu/openbook.php?record\_id=12638&page=R1.](http://www.nap.edu/openbook.php?record_id=12638&page=R1)

Bruce Katz and Robert Puentes, “Memo to the President: Invest in Long-term Prosperity,”

*Brookings Institution*, (January 12, 2009), [http://www.brookings.edu/papers/2009/0112\_prosperity\_memo.aspx.](http://www.brookings.edu/papers/2009/0112_prosperity_memo.aspx)

Bob Prieto, “Infrastructure Resiliency: Do We Have the Focus Right?”

( 2009), [http://www.tisp.org/index.cfm?cdid=11838&pid=10261.](http://www.tisp.org/index.cfm?cdid=11838&pid=10261)

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 10(3), (September 2011), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_September2011_9_11_10thAnniversary.pdf>.

**ATTACHMENT 1**

**CRITICAL INFRASTRUCURE PROTECTION AND RESILIENCE INCIDENT MANAGEMENT EXERCISE #1**

**PHYSICAL-CYBER TERRORISM SCENARIO**

**MODULE 1: PRE-INCIDENT**

**1. Scenario Build**

• A new extremist video is released on several Middle Eastern Internet sites focused on physical and cyber attacks targeting European and American interests worldwide, with a particular emphasis on energy, transportation, commercial facilities and sports venues, religious worship sites, iconic symbols, financial centers, and government buildings. The video describes “striking the infidels where they are most vulnerable,” using advanced weapons and tactics, including cyber operations.

• There is a brief mention of the video in daily news reporting; however, the general public is unaware of any threat. Government sources acknowledge the video, but take no further public action.

• Officials in the Federal republic of Germany apprehend a person described as being an “Operational Chief to multiple terrorist cells worldwide.” The man’s name is withheld, but he provides information describing future physical and cyber attacks within Europe (timing unspecified), including previously unknown connections to European cyber network “hacktivist” organizations, and admits to planning a failed attack in France late last year.

• Extremist group Internet “chatter” and Jihadi website activity are on the increase, with focused pronouncements of violent intent with near-term implications. The number of websites featuring homemade bomb-making instructions and chemical agent applications has proliferated greatly in recent months.

2. **One Month Later**

• The main multi-modal train station and several popular tourist sites are attacked in Berlin, Federal Republic of Germany. A man carrying a backpack is apprehended by German authorities after his suicide vest failed to completely detonate inside the station while awaiting the arrival of a fully loaded passenger train. The bomb injured six commuters and severely burned the suspect. The suspect is quickly taken to a local detention facility for questioning after being treated for second-degree burns at a local hospital. A second bomb explodes in a crowded plaza outside the main train station, serving as an immediate rally point for those fleeing the station. Twenty people are killed and three dozen more are wounded. Traces of the bomber’s clothing and personal effects have been found on scene, but he is believed to have been killed during the attack. It is believed that the two separate bombing incidents are linked based upon preliminary analysis of video surveillance footage taken in and around the station.

• Coincidental to the mass transit bombing, the web sites and Internet communications of several key German ministries and local agencies involved in the response and public communications were attacked and disrupted. This led to an uncharacteristically confused response and uncoordinated public messaging on the part of German authorities at all levels.

• The transit bombing suspect is identified as a militant associated with a European affiliate of the Al Qaeda organization. He states that his planned attack was to serve as a warning to all countries with “Criminals assaulting Islam.” He is quoted as saying “When the criminal governments fall, Al Qaeda will be triumphant.” The suspect has also provided information that leads to the conclusion that there are additional active cells elsewhere in Europe in the final stages of operational planning and mission rehearsal. Subsequent questioning also indicates that the suspect may have extensive ties to a number of well-financed European cyber hacktivist organizations.

• The German Government has elevated security around governmental facilities, major transportation hubs and other potential “mass gathering” targets across the country. The Berlin metro system remains open, but is operating under heightened security conditions. The German government is also conducting a coordinated investigation regarding the potential source of the targeted cyber disruptions that accompanied the mass transit bombings.

**3. Discussion Questions**

• What actions would German authorities take in response to the mass transit attack and cyber disruptions? The authorities within other European countries?

• What information would German authorities share with U.S. government counterparts at this time, regarding both the physical attack and focused cyber disruptions?

• What intelligence would be circulating domestically within the Federal government, between Federal and local authorities, and between government and the private sector?

• Are the events prior to the attack distinguishable from day-to-day intelligence and cybersecurity “white noise” from a U.S. perspective?

• Would there be any changes recommended to protective measures across the U.S. critical infrastructure sectors based on a coordinated physical-cyber malicious actor an event occurring abroad with no corresponding credible threat in the United States?

• What prevention/protection activities would your jurisdiction/agency/sector be engaged in at this time? What are your principal concerns at this time?

• What would the various key nodes of the NIPP/NRF/NCIRP incident management frameworks be doing at this time?

**MODULE 2: WARNING**

**1. Scenario Build**

• During the week after the terrorist attack on the mass transit system in Berlin, the FBI and DHS have received increased reporting of planning for possible near term attacks on commercial facilities, government facilities, national monuments, financial centers, and the transportation sector (highways, rail, ferries, and ports) across the United States.

• Exact methods and timing of these potential attacks are unknown, but the various sources from which the reporting has originated have been deemed credible.

• A tape is released on the Internet and on the Arab television network Al Jazeera by an Al Qaeda affiliate with known operations in Europe and Southwest Asia which trumpets forthcoming attacks in the United States and makes additional claims regarding the possession of unspecified “WMD” and cyber disruption capabilities.

• Several major news agencies receive phone calls from unidentified sources warning of an impending “reign of terror” and “cyber Pearl Harbor” in the United States.

• In response to this threat reporting, the FBI and DHS issue a joint intelligence bulletin warning of possible attacks against commercial facilities, government facilities, and surface transportation, and Internet systems and conduct national conference calls and provide briefings on the threat to critical infrastructure sector partners.

• The U.S. national threat alert is issued through the NTAS and the NCAS with specific emphasis on commercial facilities, national monuments, government facilities, transportation sector (highways, rail, mass transit, ferries, and ports), and the information technology sector and related information systems, as well as for the National Capital Region and New York State.

• A prominent European “hacktivist” organization reveals the existence of a vulnerability common to the industrial control systems typically employed internationally and in the U.S. within the electricity, chemical, oil and gas, and manufacturing sectors. This vulnerability is referred to as “Pandora” by the international hacker community. The Pandora vulnerability and the potential means to exploit it were principal topics of discussion at an international “hacktivist” convention held earlier this month in Amsterdam. The international media and Internet coverage of this vulnerability is widespread. Numerous extremist websites and chat rooms contain references to the Pandora vulnerability and its potential exploitation. DHS issues a warning regarding this vulnerability and its potential exploitation through the US-CERT and ICS-CERT. Additionally, ICS-CERT issues a list of potential defensive countermeasures/effective practices, including technical remediation products/solutions, vendors, and recommended security upgrades.

• There is tremendous angst among the cyber and ICS user communities regarding the recent cyber attacks in Germany and the much publicized Pandora vulnerability. Patches and other remediation measures have been employed throughout various critical infrastructure sectors, but the exact nature of the threat and extent of the Pandora vulnerability remain largely unknown. DHS and the FBI have reason to believe through numerous email intercepts that some of the security upgrades recommended to mitigate the Pandora vulnerability may have actually contained malware disguised as legitimate software, with the European hacktivist organizations with unknown ties to Al Qaeda the likely perpetrators of this tactic. The exact nature of the malware and potentially affected products affected remains unknown.

**2. Discussion Questions:**

• What are your major personal and organizational concerns at this point?

• Would there be any intelligence updates or warnings to the private sector or State and local government officials at this time? If so, how would this process work?

• How would your organization be alerted to a cyber threat?

• What are the essential elements of intelligence and related information required by your jurisdiction, agency, community, and industry to effectively deal with this scenario?

• What physical/cyber preventive/protective measures would government and the private sector put in place at this point regarding the various threat vectors in play? How would they be communicated to one another?

• What recommendations would these entities make regarding the NTAS and NCAS threat alert? How does this process work?

• In the absence of government guidance or action, would the private sector initiate any changes in protective measures and emergency response posture?

• If so, would these changes be individually considered or would industry within a sector come together and collaborate?

• What types of activities would the various key nodes of the NIPP/NRF/NCIRP incident management frameworks engage in at this point?

• How would the NIPP partnership act to better understand the nature of and take action to mitigate the unspecified “WMD” and cyber threats? Are critical infrastructure owners and operators and mass public venue security officials prepared to deal with chemical and other potential WMD threats?

• What actions would the U.S. government/industry take in response to the discovery of the Pandora ICS vulnerability? What is the specific role of the ICS-CERT and the various sector ISACs in dealing with this vulnerability?

• What types of protective measure enhancements would be implemented by the NIPP Partnership across the critical infrastructure sectors based on the Pandora vulnerability? How would the status of Pandora remediations across the sectors be monitored and evaluated?

• How would the public message regarding the various threats at play and the Pandora vulnerability be developed, coordinated, and disseminated? Who has the lead regarding public messaging and national cyber incidents?

**MODULE 3: ACTIVATION AND IMMEDIATE RESPONSE**

**1. Scenario Build**

• **Today 8:32 a.m. EDT**

o Two large rental trucks drive into the Ft. Pitt Tunnel in Pittsburgh, Pennsylvania, and explode. As a result, there are numerous unconfirmed casualty reports, and the major interstate network servicing the greater Pittsburgh area is closed except to emergency vehicles. It is later determined that 55 commuters are killed and over one hundred are injured.

• **8:35 a.m. EDT**

o An improvised explosive device (IED) is detonated in Washington, D.C.’s Capitol South Metro Station; six people are killed and 30 people are injured. The Blue and Orange Metro lines have been closed to the public inside the Beltway pending further investigation.

• **8:40 a.m. EDT**

o A backpack IED is found outside the main entrance of a crowded public shopping mall near the Pentagon in Arlington, Virginia. The IED is cordoned off and disarmed without incident. The mall and surrounding commercial businesses are temporarily closed to the public while further bomb sweeps are conducted.

• **9:00 a.m. EDT**

o In Chicago, a minivan is detained in front of the Mercantile Exchange for loitering in front of the building. Upon investigation, the minivan is found to be carrying ten unidentified “chemical” canisters packed with homemade explosives. The driver is taken into custody and held at a local FBI detainment facility. Access into the Mercantile Exchange is temporarily closed; the facility is expected to open under heightened security conditions following further bomb sweeps.

• **10:00 a.m. EDT**

o The NTAS threat level is elevated to “Imminent” for tunnels and bridges, mass transit, commercial facilities, and government facilities. All other sectors remain at an “Elevated” level under the NTAS.

• **12:00 p.m. EDT**

o Internet video is released from an Al Qaeda affiliate claiming responsibility for the attacks on the United States. The video is several minutes long and includes the following statement: “A first blow has been struck, the suffering of the oppressors has begun and their nightmare will continue. This is only the beginning. Every city of evil soon will be touched; the child of every criminal will know fear, death and darkness as our children have known them.”

• **3:00 p.m. EDT**

o The North American Electric Reliability Corporation (NERC) reports that several remote, unmanned power generating stations in the Midwest are experiencing sporadic real time generation data feed failure and faulty emergency readings on key transmission system elements for no apparent reason. Additionally, numerous substations are reporting erroneous voltage data readings.

• **6:00 p.m. EDT**

o Breakers on several transmission lines providing power to the greater Chicago area have been tripped by malfunctioning ICS components, causing a large power outage affecting major portions of the city. Industry technicians are rerouting electricity to unaffected lines, and the area power provider has begun load shedding operations, causing rolling blackouts in an area affecting half a million or so customers. These outages have affected the normal operation of the Chicago area mass transit system as well as several hundred traffic lights in congested areas of the city during the evening rush hour, causing huge traffic disruption/gridlock and mass movements of stranded commuters on foot across the impacted area. Chicago’s Midway and O’Hare Airports have also suspended operations due to the blackouts and uncertainty regarding the security of the cyber system supporting regional air traffic control operations. Local and national media area providing continuous coverage of this evolving scenario, attempting to “connect the dots” between this event and the bombing events earlier in the day. Chicago area residents are bombarding the local electric utility and city and county government emergency management offices with requests for information and assistance and assurances of their safety.

• **9:00 p.m. EDT**

o The same Al Qaeda affiliate claiming responsibility for the bombing attacks of earlier in the day issues a statement over numerous Internet websites claiming responsibility for the Chicago area power blackout. The announcement states that additional metropolitan areas of the country will be similarly affected within the next couple of days.

o Federal government authorities are coordinating with local government and private sector officials to determine the cause of the outages and jointly determine the public messaging strategy. The initial investigation finds that the power blackouts were caused by a malicious cyber intrusion of key ICS functions susceptible to the Pandora vulnerability at the substation and control center levels. No official connection has been established regarding the power outages and the bombing events earlier in the day.

o US-CERT, ICS-CERT, and their electric industry partners coordinate with one another in response to the ICS penetration and re-issue the list of Pandora defensive countermeasures/effective practices, including technical remediation products/solutions, vendors, and recommended upgrades. The NCAS is elevated to “Imminent.”

**2. Discussion Questions:**

• What are your principal concerns and priorities at this time?

• How does the “WMD Factor” complicate emergency protection and response activities?

• How would the “dots be connected” between the bombing events and the ICS-produced power blackout?

• What types of intelligence updates would be provided at this time, to whom, and by whom?

• What would be the nature of any cyber alerts/warnings provided by the Federal government to the private sector and/or State and local government officials at this time? How would this process work?

• How would the discussion related to the NTAS elevation be framed? How does this process work? What are the near and medium-term ramifications of the NRAS elevation across the affected sectors?

• What protection and emergency response actions are Federal, State, and local government and private sector authorities taking following these events?

• How is situational awareness being maintained across government and between the government and the private sector at this point?

• Do you have sufficient authorities, capacities, and resources to deal with the events above as they impact your area of responsibility? If not, where do you go for help?

• What key nodes of the NRF/NCIRP are operational at this point?

• What are the roles of the US-CERT, ICS-CERT, and NSCCCC regarding the day’s events?

• What actions are being undertaken by the sector operations centers, ISACs, or other information sharing entities?

• How would the discussion related to the NCAS elevation be framed? How does this process work?

• How would you handle internal and external messaging of the events as they pertain to you and your organization, community, jurisdiction, or sector? How is this messaging coordinated with external partners to include various levels of government and industry?

**MODULE 4: EXTENDED RESPONSE AND RECOVERY**

**1. Scenario Build**

• **Two weeks from the attacks in the United States**

o There are no additional cyber disruptions to the electric grid following the Chicago area blackout. Through subsequent investigation, the FBI has established a positive connection between the Chicago area malicious ICS activities and the bombing events that occurred earlier that day. The exact nature of this connection in not known in any great detail; nor is the exact nature of the technical capability ascribed to the perpetrator.

o DHS releases a statement from the Secretary lowering the NTAS threat level but maintaining a level of “Elevated” for government facilities, commercial facilities, the transportation sector (highways, rail, ferries, mass transit, ports and airports). The NCAS remains at “Elevated” for the indefinite future.

o The FBI announces that they have arrested three men associated with the IED attacks and that their investigation will continue. At least one of the men is believed to be connected to the Berlin mass transit bombings as well.

o The national and international impacts of the terrorist attacks in the United States and the Chicago area power blackout have been extraordinarily high, cascading across the sectors domestically and internationally. The stock market has fallen to recession levels, with downward trends globally.

o State and local officials have severely taxed their local first responder communities over the course of the period of heightened alert following the attacks and power blackout. Private sector security and emergency preparedness and response forces have been similarly stressed. The costs of a “new threshold for physical and cybersecurity” are being felt to varying degrees across the sectors.

o Public messaging across levels of government has been fairly consistent in the two weeks following the attacks. Public confidence remains low and apprehension regarding follow-on attacks and cyber disruptions remains high.

• **Three weeks from the attacks in the United States**

o DHS releases a statement from the Secretary lowering the national threat level for all sectors.

o Pipe bombs are found at a high school in Chicago, Illinois. Two students are arrested.

o There are numerous media reports of other threats involving the use of IEDs being reported to local authorities ranging from attacks against transit, schools, commercial facilities, and national monuments and icons. Public apprehension remains high.

o The official websites of the NERC and Department of Energy were taken off line for a day by a malicious cyber intrusion. No organization has claimed responsibility for this disruption.

**2. Discussion Questions:**

• What are your principal concerns in this phase of incident management? What are your long-term concerns/issues associated with the terrorist bombings and cyber disruptions?

• What types of enhanced information sharing and prevention and protection activities would you continue at this point? Do you have sufficient resources? If not, where do you go for help?

• What impacts have the various changes in the NTAS/NCAS threat level had on your organization/constituency?

• What is the “new normal” for your agency, jurisdiction, corporation, and sector at this point? How do you resume your operations?

• What are the long-term economic and psychological implications of the attacks from your perspective?

• How do we regain public confidence in the aftermath of the attacks and into the future?

• What are the major lessons that you have learned from this exercise?

**ATTACHMENT 2**

**CIPR INCIDENT MANAGEMENT EXERCISE #2**

**HURRICANE SCENARIO**

**MODULE 1: 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. 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.

**2. 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?

• 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?

• 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?

• What are the most significant concerns of the agency/organization that you represent at this stage of hurricane season?

**MODULE 2: 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.

**2. 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 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, 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?

• What key nodes of the NRF CIKR 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 3: LANDFALL (H-HOUR)**

**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:

o Over 4M customers are without power in the region, to include numerous major hospitals and special needs facilities.

o Numerous major transformer towers are down in SW Louisiana.

o Major rail and highway networks are shut down and/or damaged.

o The I-10 bridge across Lake Pontchartrain has been dismembered in several places; other secondary and tertiary bridges are down throughout the region.

o Two major nuclear power plants in the region have suffered minor damages, but have been placed in shut down mode.

o Over a dozen major oil and natural gas pipelines are inoperative, with extent of damages unknown.

o More than one hundred Gulf oil platforms have been evacuated; several are now “free-floating.”

o Six major oil refineries in the region have been extensively damaged and will require long repair times.

o Cellular communications have been significantly degraded throughout the region; cell towers are down across the area.

o 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.

o 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.

o Gasoline is in short supply across the region; first responder operations have priority.

o 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, and damage assessment 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 CIKR 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 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? Volunteers who have the best interest at heart, but are not following the rules?

• How are critical infrastructure restoration priorities determined by government and industry at this point?

• 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 4: POST-LANDFALL TO RECOVERY (2 DAYS TO 2 MONTHS 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 leaks are prevalent throughout the area.

• Long-term impacts to the regional transportation network and power grid are extensive. Over 2.5M customers remain without power for weeks into the event.

• 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 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?

• 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?

• Does the NIPP framework adequately address long term recovery issues?

• 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.)?