

**Course Number: XXXX**

**Capstone Seminar in Critical Infrastructure Protection 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 introductory course of this series, the 21<sup>st</sup> 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 infrastructures 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 public and private sectors at all levels.

Federal agencies, States, regions and local agencies 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 infrastructures of concern 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 critical infrastructure protection and resilience. 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.

This course is a 15-lesson graduate-level seminar providing an advanced focus on critical

infrastructure protection 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 protection and resilience field. As such, it is targeted toward mid-career public and private sector professionals and members of the policy and academic communities with roles and responsibilities related to critical infrastructure protection and resilience strategy development, planning, training, program management, and incident management operations. It is also targeted toward learners who have completed pre-requisite courses in the critical infrastructure series.

This course is designed according to a building block approach, intended to foster the development of an advanced baseline of relevant knowledge among seminar participants and apply this baseline to “hands-on” critical infrastructure protection and resilience strategy and plan development and in-classroom incident management exercises. It begins with an examination of the strategic context presented by the 21<sup>st</sup> century risk environment, various critical infrastructure protection and resilience policy and planning frameworks, and operational landscape across sectors and governmental jurisdictions, vertically and horizontally. It also examines the constituent elements of critical infrastructure protection and resilience strategy development, planning, program management, and incident management, including the following: public-private partnership networks, information-sharing regimes, risk analysis and prioritization, risk mitigation, performance metrics, and incident management coordinating structures.

Working within the collective framework represented by these elemental building blocks, the course addresses the fundamentals of comprehensive critical infrastructure protection and resilience strategy and plan development at the Federal, State, tribal, and local levels of government, as well as at the sector and corporate levels within the private sector. The course concludes with an interactive module focused on the complexities of critical infrastructure protection and resilience incident management operations from an all-hazards perspective.

This course is designed to promote advanced subject-matter understanding, critical issue analysis, and insight into senior leader risk assessment, decision making, and planning processes. It also includes a comprehensive practical examination of critical infrastructure protection and resilience stakeholder interaction and key subject-matter areas through a collaborative planning project, interactive tabletop exercises, and an oral presentation. This course promotes an advanced understanding of the various applications of critical infrastructure protection and resilience strategies, plans, and incident management structures and coordinating processes across the Nation’s 18 critical infrastructure sectors.

**CREDITS CONFERRED: 3**

**PREREQUISITE: Course Number XXXX: Introduction to Critical Infrastructure Protection and Resilience**

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

This course is designed to enable learners to:

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

- Course introduction and overview; framing principles and concepts
- Review of the historical evolution of critical infrastructure protection and resilience as a national policy area; overarching policy approaches and implications for critical infrastructure protection and resilience stakeholder community 1996-present
- Review of Congressional engagement in the critical infrastructure policy area post 9-11 and post-Katrina
- Re-examination of the 9-11 Attacks, Hurricane Katrina, Gulf oil disaster, and international cyber intrusions as “broad-brush” focusing events

**2. Promote an advanced understanding of critical infrastructure protection 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 Protection at the State, Regional, Local, tribal, and territorial Level
- Regional Resilience Handbook
- Corporate security, emergency response, and business continuity plans

**3. Promote an advanced understanding of the 21<sup>st</sup> century risk environment in the context of the critical infrastructure protection and resilience mission area:**

- Threats: terrorism, cyber attacks, natural disasters and naturally occurring phenomena, industrial accidents and other manmade events, other emergencies
- Vulnerabilities (facility, node, system level)
- Consequences (public health and safety, economic loss/disruption, continuity of government and essential services, iconic loss, etc.)
- Cross-sector dependencies/interdependencies issues
- Informing executive and managerial decision-making related to critical infrastructure protection and resilience plans and programs

**4. Advance familiarity with the authorities, roles, responsibilities, and capacities of key public and private sector stakeholders with critical infrastructure protection and resilience responsibilities:**

- Federal, State, tribal, local, territorial, private sector, and international
- Touch points and flash points
- Regulations, incentives, and motivations

**5. Develop an advanced understanding of the building blocks of critical**

**infrastructure protection and resilience strategy development, planning, and incident management operations:**

**a. Critical infrastructure protection and resilience partnership frameworks, information sharing processes/systems, and coordination/collaboration structures:**

- Federal, State, tribal, local, territorial, private sector, and international partner collaboration, coordination, and communication
- Critical infrastructure data collection, warehousing, and protection
- All-hazards information sharing
- Challenges and opportunities

**b. Critical infrastructure protection and resilience risk analysis, risk mitigation, and performance measurement:**

- Physical security
- Cybersecurity
- Insider Threats
- Resilience
- Systems dependencies/interdependencies
- Regional risk frameworks
- Sector considerations

**c. Critical infrastructure Sector-level Approaches:**

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Postal and Shipping
- National Monuments and Icons
- Nuclear Reactors, Materials, and Waste
- Healthcare and Public Health
- Transportation Systems
- Water
- Information Technology

**6. Develop a practical understanding of critical infrastructure protection 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 protection and resilience goals, objectives, risk mitigation approaches/plans, and measures of performance
- Designing and applying continuous feedback mechanisms to measure critical infrastructure protection and resilience program performance
- Designing and implementing critical infrastructure protection and resilience awareness, education, and training plans and programs
- Achieving critical infrastructure protection and resilience in a resource constrained environment
- Planning for the future risk and critical infrastructure operational environments

**7. Develop an advanced understanding of and practical familiarity with the national critical infrastructure protection 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
- 9/11 Attacks
- Madrid/London Transit Bombings
- Hurricane Katrina
- California Wildfires
- Mumbai Attack
- 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, Congressional Research Service, 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 and multiple perspectives.

**GRADING:**

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

## ORAL/WRITTEN REQUIREMENTS:

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

Learners will work collaboratively in 2-3 person teams to develop a critical infrastructure protection and resilience strategy, plan, or program targeted at the corporate (enterprise level), sector, jurisdictional (Federal, State, local, tribal, 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*, or a recognized corporate-level business continuity plan.

Each team will present the highlights of its critical infrastructure protection and resilience 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 one hour 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 not later than the beginning of class on Lesson 3.**

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

Learners will participate in two role-based, interactive tabletop exercises. The first will simulate a complex, well-coordinated 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 preparations for and the 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 student will be assigned a role as a key public or private sector official with attendant critical infrastructure concerns and responsibilities. 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 on **Lesson 3**.

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

Participation includes coming to class prepared, engaging in class discussions, being a full partner in group activities, and dynamic role playing during the critical infrastructure protection 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 student 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 additional suggested readings accessible on-line, with website addresses provided in the lesson description section that follows below.

Ted G. Lewis (editor), *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, John Wiley & Sons, Inc., 2006.

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

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

## COURSE OUTLINE

### **LESSON 1 TOPIC: COURSE OVERVIEW AND INTRODUCTION TO ADVANCED CONCEPTS IN CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE**

#### **1. Lesson Goals/Objectives:**

- Become familiar with the scope of course, administrative requirements, instructional methodology, evaluation criteria, and feedback processes
- Review the evolution of critical infrastructure as a national policy focus area, 1996-present
- Develop an advanced understanding of the various statutes and Presidential policy documents governing the application of critical infrastructure protection and resilience in the United States, including their application to strategy development and planning
- Develop an advanced practical understanding of how critical infrastructure protection and resilience policies and plans have evolved as a function of the all-hazards risk environment
- Understand why the definition of “critical infrastructure” and the scope of the critical infrastructure protection and resilience sector-focused construct have changed over time
- Review the general critical infrastructure operational landscape across the sectors and the U.S. 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?
- What are the principal variations across sectors regarding critical infrastructure?
- Why does critical infrastructure protection and resilience represent such a challenge within and across governmental jurisdictions and sectors?
- What are the general principles we typically associate with critical infrastructure protection and resilience in the U.S. context?
- How does policy support strategy and plan development for critical infrastructure protection 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 protection and resilience preparedness and planning changed over time and with regard to certain threats/hazards?
- What are the differences between and what are the strengths and weaknesses of the various Presidential policies focused on critical infrastructure protection and resilience over the last 15 years?
- How does the U.S. Congress view the critical infrastructure protection and resilience mission area? Does legislation clarify or complicate the critical infrastructure protection and resilience mission space?
- Where should the next Administration/Congress take the critical infrastructure

protection and resilience mission area?

**3. Required Reading:**

Lewis, Chapters 1&2.

Collins and Baggett, Chapters 1-3.

Congressional Research Service Report, *Critical Infrastructures: Background, Policy, and Implementation*, June 2010, [http://assets.opencrs.com/rpts/RL30153\\_20100607.pdf](http://assets.opencrs.com/rpts/RL30153_20100607.pdf).

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

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

Homeland Security Presidential Directive-7, *Critical Infrastructure Identification, Prioritization and Protection*, 2003, [http://www.dhs.gov/xabout/laws/gc\\_1214597989952.shtm#1](http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1).

*National Infrastructure Protection Plan*, Executive Summary, Chapters 1&5, 2009, [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

U.S. Department of Homeland Security, *Quadrennial Homeland Security Review Report, 2010*, [www.dhs.gov/xlibrary/assets/qhsr\\_report.pdf](http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf).

**4. Additional Recommended Reading:**

*National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 2003, [http://www.dhs.gov/xlibrary/assets/Physical\\_Strategy.pdf](http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf).

*National Strategy for Homeland Security*, 2007, [http://www.dhs.gov/xlibrary/assets/nat\\_strat\\_homelandsecurity\\_2007.pdf](http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf).

## **LESSON 2 TOPIC: INTRODUCTION TO CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE STRATEGY AND PLANNING FRAMEWORKS**

### **1. Lesson Goals/Objectives:**

- Gain an advanced understanding of in-place and evolving critical infrastructure protection and resilience strategy and planning frameworks: Federal, State, local, tribal, and territorial government approaches; regional approaches; and private sector approaches
- Become familiar with major efforts to develop and implement critical infrastructure protection and resilience and business continuity strategies and initiatives at the Federal, State, tribal, territorial, and local level, as well as across the private sector
- Become familiar with concepts of “prevention,” “protection,” and “resilience” as they relate to the critical infrastructure protection and resilience mission area
- Become familiar with the concept of “community resilience” as it relates to critical infrastructure protection and resilience planning

### **2. Discussion Topics:**

- What are the major planning frameworks that guide preparedness and planning and critical infrastructure protection 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 protection and resilience mission? How does business continuity planning relate to critical infrastructure protection and resilience? How do the public and private sectors interact in the critical infrastructure protection and resilience and business continuity planning processes?
- What is the concept of “Resilience” and how does it apply in the context of critical infrastructure protection and resilience planning?
- What are the general principles associated with resilience as currently approached by government and industry?
- How do we achieve an appropriate balance between prevention, protection, and resilience in the context of critical infrastructure protection 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 recommendation?

### **3. Required Reading:**

U.S. Department of Homeland Security, *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal and Territorial Level*, 2008,

**(General review only).**

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

*Business Continuity Plan Template*,  
<http://www.ready.gov/business/downloads/sampleplan.pdf>.

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

Dr. Jim Kennedy. *Critical Infrastructure Protection is all About Operational Resilience*, 2006, <http://www.continuitycentral.com/feature0413.htm>.

Brandon J. Hardenbrook, *The Need for a Policy Framework to Develop Disaster Resilient Regions*, 2005, <http://www.bepress.com/jhsem/vol2/iss3/2/>.

T.D. O'Rourke, *Critical Infrastructure, Interdependencies and Resilience*, 2007, <http://www.members.nae.edu/nae/bridgecom.nsf/weblinks/CGOZ-6ZQQRH?OpenDocument>.

Congressional Research Service, *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>.

Brian. Jackson, *Marrying Prevention and Resiliency*, 2008, [http://www.rand.org/pubs/occasional\\_papers/2008/RAND\\_OP236.pdf](http://www.rand.org/pubs/occasional_papers/2008/RAND_OP236.pdf).

U.S. Government Accounting Office, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, October 2007, <http://www.gao.gov/new.items/d08212t.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>.

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).

Public Safety Canada, *National Strategy for Critical Infrastructure and Action Plan for Critical Infrastructure*, 2010, <http://www.publicsafety.gc.ca/prg/em/ci/ntnl-eng.aspx>.

**LESSON 3 TOPIC: EXAMINING CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE STRATEGY AND PLANNING IN THE CONTEXT OF THE 21<sup>ST</sup> CENTURY RISK ENVIRONMENT**

**\*\*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:**

- Develop an advanced understanding of the various all-hazards threats that may impact critical infrastructure across the 18 critical sectors and on a regional basis nationwide
- Understand the evolving nature of the terrorist threat as it applies to critical infrastructure protection and resilience strategies and plans
- Become familiar with various real-world situations in which critical infrastructures were dramatically impacted by manmade or naturally occurring threats and hazards
- Become familiar with the challenges associated with critical infrastructure protection and resilience planning in the current and projected threat environment

**2. Discussion Topics:**

- Currently, what are the principal threats to our critical infrastructure assets, systems, and networks?
- What part does our critical infrastructure “target sets” play in the concept of “asymmetric warfare?”
- How has the nature of the threat to our critical infrastructure evolved over time?
- Why do critical infrastructure assets, systems, and networks represent preferred targets for malicious actors (international terrorists, domestic terrorists, criminal organizations, etc.)?
- What are the principal challenges we face in ensuring the protection and resilience of our critical infrastructure in light of these threats?
- How does the threat impact strategy and plan development in this mission area?
- How are threat assessments accomplished and communicated within and across the various levels of government and the private sector?
- What are the trends regarding international terrorist acts focused on critical infrastructure assets, systems, and networks outside the United States? Are there lessons to be learned from these experiences?
- Are our critical infrastructures more resilient in a post-Katrina world? The evolving world of the future?
- Can we afford the cost of maintaining an all-hazards critical infrastructure preparedness posture?

**3. Required Reading:**

Lewis, Chapter 3 and Chapter 13, pp. 397-401.

Collins and Baggett, Chapters 13-15.

Congressional Research Service Report, *International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress*, March 18, 2010, <http://www.fas.org/sgp/crs/terror/R41004.pdf>.

Congressional Research Service Report, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*, February 5, 2010, <http://www.fas.org/sgp/crs/terror/R41070.pdf>.

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

Rand Corporation, *The Lessons of Mumbai*, 2009, [http://www.rand.org/pubs/occasional\\_papers/2009/RAND\\_OP249.pdf](http://www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf).

Brian Jackson and David Frelinger, *Emerging Threats and Security Planning*, 2009, [http://www.rand.org/pubs/occasional\\_papers/2009/RAND\\_OP256.pdf](http://www.rand.org/pubs/occasional_papers/2009/RAND_OP256.pdf).

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

Comfort and Haase, *Communication, Coherence and Collective Action: The Impact of Hurricane Katrina on Communications Infrastructure*, 2006, [http://www.iisis.pitt.edu/publications/Communication\\_Coherence\\_and\\_Collective\\_Action-Katrina.pdf](http://www.iisis.pitt.edu/publications/Communication_Coherence_and_Collective_Action-Katrina.pdf).

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

**LESSON 4 TOPIC: CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE**  
**PLANNING FOUNDATIONS: AUTHORITIES, ROLES AND RESPONSIBILITIES OF FEDERAL, STATE, LOCAL AND PRIVATE SECTOR PARTNERS**

**1. Lesson Goals/Objectives:**

- Review the authorities, roles and responsibilities of government (Federal, State, tribal, territorial, local, and international) and the private sector regarding critical infrastructure protection and resilience
- Develop an advanced understanding of the differences between regulated and voluntary critical infrastructure protection and resilience regimes across the critical sectors
- Review the roles that nongovernmental organizations, the scientific/technology community, and academia play in critical infrastructure protection and resilience
- Develop an advanced understanding of the principal political, organizational, legal, and resource challenges that those responsible for critical infrastructure protection and resilience face in executing those responsibilities

**2. Discussion Topics:**

- Who is “in charge” of critical infrastructure protection and resilience nationally, regionally, locally, and across the 18 critical sectors? How is critical infrastructure protection 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 protection and resilience?
  - Federal, State, tribal, and local 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 protection and resilience planning roles and responsibilities?
- How do the various government and private entities with critical infrastructure protection and resilience responsibilities at different levels interact and collaborate with one another?
- How are the 18 critical infrastructure sectors organized to accomplish the critical infrastructure protection and resilience mission at the sector and sub-sector level? 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 protection 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. Required Reading:**

*Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization and Protection, 2003,*

[http://www.dhs.gov/xabout/laws/gc\\_1214597989952.shtm#1](http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1).

*National Infrastructure Protection Plan*, Chapter 2 and Appendices 2&5, 2009,  
[http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

U.S. Department of Homeland Security, *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal and Territorial Level*, 2008,  
[http://www.dhs.gov/xlibrary/assets/nipp\\_srtltd\\_guide.pdf](http://www.dhs.gov/xlibrary/assets/nipp_srtltd_guide.pdf).

Ken Schnepf, *Council Aims to Coordinate State/local Security Efforts*, 2007,  
<http://www.plantservices.com/articles/2007/198.html>.

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

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

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

**LESSON 5 TOPIC: APPROACHES TO ORGANIZING AND PARTNERING FOR CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE AND NETWORKING TO SHARE INFORMATION**

**1. Lesson Goals/Objectives:**

- Review the structures, processes, and coordinating mechanisms associated with the NIPP Partnership Model
- Develop an advanced understanding of the nature of collaborative interaction between the Sector Coordinating Councils, Government Coordinating Councils, and Regional Consortium Coordinating Council under the NIPP framework
- Review the various methods, processes, and systems that the various critical infrastructure protection and resilience partners use to share information with one another
- Develop an advanced understanding of the ongoing challenges and barriers to information sharing and collaboration that exist between the various levels of government and the private sector
- Review 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 protection and resilience strategies and plans?
- How does one go about the process of building a public-private partnership network or coalition for critical infrastructure protection 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 protection and resilience community?
- 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 protection 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 protection 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 protection and resilience mission?
- What are the key processes and systems used to share critical infrastructure protection 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 protection and resilience information sharing and analysis?
  - How is information and intelligence that originates from multiple distributed sources compiled and deconflicted? Are we successfully “connecting the dots” today?
  - How does information sharing factor into critical infrastructure protection and resilience strategy and planning efforts?
  - How does the President’s new mandate of “no lobbyist” in SCC affect the NIPP partnership?
  - What does resilience really mean? Are some sectors more resilient than others by nature or construct?

### **3. Required Reading:**

*National Strategy for Information Sharing*, 2007,  
<http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html>.

*National Infrastructure Protection Plan*, Chapter 4 and Appendices 5a&b, 2009,  
[http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

Robert Riegle, Testimony, *The Future of Fusion Centers: Potential Promise and Dangers*, 2009, [http://www.dhs.gov/ynews/testimony/testimony\\_1238597287040.shtm](http://www.dhs.gov/ynews/testimony/testimony_1238597287040.shtm).

State, Local, Tribal and Territorial Coordinating Council, *Critical Infrastructure and Key Resource Protection Capabilities for Fusion Centers*, July 2008, In U.S. Department of Homeland Security, *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal and Territorial Level*, 2008.

*Information Sharing Environment*,  
[http://itlaw.wikia.com/wiki/Information\\_Sharing\\_Environment](http://itlaw.wikia.com/wiki/Information_Sharing_Environment).

*The Role of ISACs in Private/Public Sector CIP*, 2009,  
[http://fsisac.us/index.php?option=com\\_docman&task=cat\\_view&gid=40&limit=15&limitstart=0&order=hits&dir=DESC&Itemid=208](http://fsisac.us/index.php?option=com_docman&task=cat_view&gid=40&limit=15&limitstart=0&order=hits&dir=DESC&Itemid=208).

*A Policy Framework for the ISAC Community*, 2004,  
[http://www.isaccouncil.org/index.php?option=com\\_docman&task=doc\\_view&gid=13&Itemid=208](http://www.isaccouncil.org/index.php?option=com_docman&task=doc_view&gid=13&Itemid=208).

Department of Homeland Security, State and Local Fusion Centers, September 16, 2009,  
[http://www.dhs.gov/files/programs/gc\\_1156877184684.shtm](http://www.dhs.gov/files/programs/gc_1156877184684.shtm).

U.S. Government Accountability Office, *Homeland Security: Federal Efforts are Helping to Address Some Challenges Faced by State and Local Fusion Centers*, 2008, <http://www.gao.gov/new.items/d08636t.pdf>.

*Information Sharing and the Private Sector*,  
<http://www.ise.gov/Pages/sharingprivatesector.aspx>.

**3. Recommend Additional Reading:**

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](http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf).

R.A. Best, *Sharing Law Enforcement and Intelligence Information: The Congressional Role*, Congressional Reporting Service RL 33873, 2007,  
<http://www.fas.org/sgp/crs/intel/RL33873.pdf>.

CIKR Resource Center, *CIKR Partnerships*,  
<http://training.fema.gov/EMIWeb?IS/IS860a?CIKR/CIKRpartnerships.htm>.

**LESSON 6 TOPIC: THE KEY TO CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE STRATEGY AND PLAN DEVELOPMENT: ASSESSING CRITICAL INFRASTRUCTURE RISK IN AN INTERDEPENDENT WORLD**

**1. Lesson Goals/Objectives:**

- Develop an advanced understanding of the major elements of risk in the context of critical infrastructure protection and resilience planning: threats, vulnerabilities, and consequences
- Develop an advanced understanding of how the elements of risk relate to the human, physical, and cyber aspects of critical infrastructure protection and resilience
- Be able to critique the DHS strategic risk assessment process, as well as how other government and private sector critical infrastructure stakeholders view and evaluate risk
- Develop an advanced understanding of the complexities regarding critical infrastructure dependencies and interdependencies as they relate to risk
- Examine how risk drives (or does not drive) risk management strategies, plans, and resource investment across government and the private sector

**2. Discussion Topics:**

- What are the major elements of risk as they pertain to the critical infrastructure protection and resilience mission? How are they quantified to support risk management decisions?
- 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 protection and resilience relate to the concept of risk?
- Do the vulnerability assessment processes used to help define risk within the critical sectors and high-risk jurisdictions include a systemic perspective? Do these processes adequately address cross-sector and cross-jurisdictional dependencies/interdependencies issues?
- 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 protection 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 protection 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?

### **3. Required Reading:**

Collins and Baggett, Chapter 5.

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

*National Infrastructure Protection Plan*, Chapter 3 and Appendix 3.

Congressional Research Service, *What Makes Infrastructure Critical?*

[http://www.libertysecurity.org/IMG/pdf/CRS\\_Report - What makes an Infrastructure Critical - 30.08.2002.pdf](http://www.libertysecurity.org/IMG/pdf/CRS_Report_-_What_makes_an_Infrastructure_Critical_-_30.08.2002.pdf).

George Mason University, *Critical Infrastructure Protection: Elements of Risk*, Chapter 2 “Intelligence Analysis for Strategic Risk Assessments,” 2007,

[http://www.steelcityre.com/documents/RiskMonograph\\_1207.pdf](http://www.steelcityre.com/documents/RiskMonograph_1207.pdf).

George Mason University, *Critical Infrastructure Protection: Elements of Risk*, Chapter 3 “The Meaning of Vulnerability in the Context of Critical Infrastructure Protection,” 2007,

[http://www.steelcityre.com/documents/RiskMonograph\\_1207.pdf](http://www.steelcityre.com/documents/RiskMonograph_1207.pdf).

U.S. Government Accountability Office, *Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security*, 2008,

<http://www.gao.gov/products/GAO-08-904T>.

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

[http://assets.opencrs.com/rpts/RL33206\\_20080912.pdf](http://assets.opencrs.com/rpts/RL33206_20080912.pdf).

Rinaldi, Peerenbloom, and Kelly, *Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies*, 2004,

<http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf>.

National Academy of Sciences, *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),

**LESSON 7 TOPIC: ENABLING PROTECTION, MANAGING RISK, AND MEASURING PERFORMANCE THROUGH REGULATION**

**1. Lesson Goals/Objectives:**

- Review those sectors in which security is a function of government regulatory oversight
- Develop an advanced understanding of 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
- Understand the strengths and weaknesses of the regulatory approach to critical infrastructure protection and resilience
- Become familiar with the differences in the approaches used in the sectors subject to government security regulations: chemical/hazardous materials, freight rail, aviation, ports, commercial nuclear facilities, electricity, and banking and finance
- Understand the relationship between a regulator and regulated party in the context of critical infrastructure protection and resilience
- Understand how the public-private regulatory relationship affects the planning and performance measurement processes

**3. 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 protection and resilience?
- Is there one or 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?

**3. Required Reading:**

Collins and Baggett, Chapters 6, 7, 9.

Blank Rome, *Rail Security Regulations*, 2008,

<http://www.blankrome.com/index.cfm?contentID=37&itemID=1770>.

Public Law 107-295, *Maritime Transportation Security Act of 2002*,  
<http://www.homeport.uscg.mil>.

*Security Spotlight*, 2008, (and other security references)  
<http://www.nrc.gov>.

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

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

Electronic Code of Federal Regulation, *Rail Transportation Security*, 2009,  
<http://ecfr.gpoaccess.gov>.

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

Paul Parfomak, *Pipeline Safety and Security: Federal Programs*, 2008,  
<http://www.fas.org/sgp/crs/homesec/RL33347.pdf>.

**LESSON 8 TOPIC: ENABLING PROTECTION, MANAGING RISK, AND MEASURING PERFORMANCE IN A VOLUNTARY PARADIGM**

**1. Lesson Goals/Objectives:**

- Review those sectors in which security is a function of public-private sector voluntary collaboration and coordination
- Develop an advanced understanding of how risks are assessed and managed and how performance is evaluated in those sectors in which security is not regulated by a government entity
- Understand the strengths and weaknesses of the voluntary approach to critical infrastructure protection and resilience
- Review the differences in the approaches used in the sectors that are not subject to government security regulations
- Understand the relationship between the government at all levels and the private sector in a voluntary security construct
- Understand the concepts and methods underpinning the DHS voluntary private sector preparedness program (PS-Prep)

**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 protection 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?
- 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. Required Reading:**

Collins and Baggett, Chapters 8 and 9.

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

*National Infrastructure Protection Plan*, 2009,  
[http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

U.S. Department of Homeland Security, Private Sector Preparedness Standards Program,  
<http://www.fema.gov/privatesectorpreparedness/>.

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

U.S. General Accounting Office, *Passenger and Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts*, 2007,  
<http://www.gao.gov/products/GAO-07-583T>.

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

Bill Johnstone, *New Strategies to Protect America: Terrorism and Mass Transit after London and Madrid*, 2007, [http://www.americanprogress.org/kf/transit\\_security.pdf](http://www.americanprogress.org/kf/transit_security.pdf).

Daniel Prieto, *Mass Transit after the London Bombings*,  
[http://belfercenter.ksg.harvard.edu/files/mass\\_transit\\_testimony\\_prieto\\_aug\\_4\\_2005.pdf](http://belfercenter.ksg.harvard.edu/files/mass_transit_testimony_prieto_aug_4_2005.pdf).

U.S. Government Accounting Office, *Surface Transportation Security: TSA Has Taken Action to manage Risk, Improve Coordination, and Measure Performance, but Additional Actions Would Enhance Its Effort*, April 2010,  
<http://www.gao.gov/new.items/d10650t.pdf>.

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

**\*\*Additional Readings (See below for special instructions)**

*NIPP Sector Specific Plans* (Agriculture and Food, Banking and Finance, Communications, Defense Industrial Base, Energy, Information Technology, National Monuments and Icons, Transportation and Water) located at  
[http://www.dhs.gov/xprevprot/programs/gc\\_1179866197607.shtm](http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm).

**\*\*Special Activity: Learners will read and be prepared to informally discuss/critique one of the above sector plans in detail in class. Learners will be assigned a sector plan for focus by the instructor at the end of class on Lesson 7.**

## **LESSON 9 TOPIC: INFORMATION SECURITY AND INDUSTRIAL CONTROL SYSTEMS RISK PLANNING AND PERFORMANCE MEASUREMENT**

### **1. Lesson Goals/Objectives:**

- Develop an advanced understanding of the nature of the cyber threats and challenges that impact the critical infrastructure protection and resilience mission area
- Understand the linkages between cybersecurity and critical infrastructure protection and resilience from an operational and security perspective
- Understand the authorities, capacities, and resources landscape of the cyber domain as they pertain to critical infrastructure protection and resilience
- Understand the challenges represented by information technology and Supervisory Control and Data Acquisition (SCADA) systems vulnerabilities
- Understand how cyber risk is assessed and managed within the various critical infrastructure sectors, as well as how cyber security performance is evaluated
- Understand how the cyber dimension factors into critical infrastructure protection and resilience strategies and plans within and across government and industry

### **2. Discussion Topics:**

- What are the principal threats and challenges of cyber security as they pertain to critical infrastructure protection and resilience? Is this a “real and present danger?” Why or why not?
- How does the White House Cyber Security Review Report, issued in 2009, address the cyber problem? Is this an effective approach?
- What is SCADA? How do cyber and SCADA 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 SCADA 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 SCADA 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 protection and resilience-focused strategies and plans?
- How is planning in the cyber domain different from conventional domains?

### **3. Required Reading:**

Collins and Baggett, Chapter 10.

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

Peter Allor, *Understanding and Defending Against Foreign Cyber Threats*, 2007, <http://www.homelandsecurity.org/journal/Default.aspx?oid=165&ocat=1>.

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

U.S. Government Accountability Office, *Critical Infrastructure Protection: DHS Needs to Better Address its Cyber Security Responsibilities*, 2008, <http://www.gao.gov/products/GAO-08-1157T>.

U.S. Government Accountability Office, *Cyber security: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats*, 2010, <http://www.gao.gov/new.items/d10834t.pdf>.

U.S. Government Accountability Office, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, 2004, <http://www.gao.gov/new.items/d04354.pdf>.

Stamp, Campbell, DePoy, Dillinger, and Young, *Sustainable Security for Infrastructure SCADA*, 2003, <http://www.sandia.gov/scada/documents/SustainableSecurity.pdf>

David Watts, *Security and Vulnerability in Electric Power Systems*, <http://eric.purpletree.org/file/PaperECE723v39Format.pdf>.

Water Sector Coordinating Council, *Roadmap to Secure Control Systems in the Water Sector*, March 2008, <http://www.nawc.org/policy-issues/utility-security-resources/Final%20Water%20Security%20Roadmap%2003-19-08.pdf>.

Mariana Hentea, *Improving Security for SCADA Control Systems*, 2008, <http://ijikm.org/Volume3/IJIKMv3p073-086Hentea361.pdf>.

#### **4. Additional Recommended Reading:**

Stouffer, Falco and Kent, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrialized Control Systems Security*, 2006, [http://www.cyber.st.dhs.gov/docs/NIST%20Guide%20to%20Supervisory%20and%20Data%20Acquisition-SCADA%20and%20Industrial%20Control%20Systems%20Security%20\(2007\).pdf](http://www.cyber.st.dhs.gov/docs/NIST%20Guide%20to%20Supervisory%20and%20Data%20Acquisition-SCADA%20and%20Industrial%20Control%20Systems%20Security%20(2007).pdf).

## **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 as it relates to critical infrastructure protection 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 on Lessons 11&12. These TTXs will highlight incident management roles, responsibilities, coordinating structures and interaction between Federal, State, tribal, territorial, and local 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 protection and resilience-related communication and information sharing, coordination, integration of capabilities, and problem identification and resolution.

### **1. Lesson Goals/Objectives:**

- Understand the roles and responsibilities of government and private sector entities in the context of an emergent threat as well as an incident in progress
- Become familiar with key critical infrastructure protection and resilience incident management nodes, coordinating structures and processes through which the various public and private sector stakeholders interact as discussed in the *National Response Framework* and its *CIKR Support Annex* — prevention and protection through response and recovery
- Understand effects upon and anticipated critical infrastructure sector actions resulting from changes in the national threat level through the National Terrorism Advisory System (NTAS) and in response to an emergent naturally occurring threat
- Become familiar with and assess public-private sector information sharing and intelligence networks in the context of incident management
- Become familiar with the processes and mechanisms used to build critical infrastructure situational awareness and facilitate public-private prevention, protection, 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?
- What are the key government and private sector incident management nodes and coordinating structures as detailed in the NIPP and the *National Response Framework*?
- How are information and intelligence shared between the various public and private sector nodes of the NIPP Partnership Framework in an emergent threat scenario? Does the process work?
- How does the recent change from the Homeland Security Advisory System (HSAS) to the NTAS affect critical infrastructure -related incident response? What actions do the sectors take in response to a national level NTAS elevation 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?
- How are private sector requests for assistance assessed and addressed during incident response operations?

### **3. Required Reading:**

*National Infrastructure Protection Plan*, Chapter 5.

National Infrastructure Advisory Council, *Framework for Dealing with Disasters and Related Interdependencies*, July 2009,  
[http://www.dhs.gov/xlibrary/assets/niac/niac\\_framework\\_dealingwithdisasters\\_slides.pdf](http://www.dhs.gov/xlibrary/assets/niac/niac_framework_dealingwithdisasters_slides.pdf)

Boin, Arjen, and Denis Smith, "Terrorism and Critical Infrastructures: Implications for Public-Private Crisis Management," *Public Money & Management* 26, no. 5 (2006), 295-304. [http://www.cipfa.org.uk/pt/pmm/download/sample\\_article.pdf](http://www.cipfa.org.uk/pt/pmm/download/sample_article.pdf).

*National Response Framework*, 2008,  
<http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.

*Critical Infrastructure/Key Resource Support Annex to the National Response Framework*, 2008, <http://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf>.

### **4. Additional Recommended Reading**

*National Incident Management System*, 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 (Public Law 93-288)*,  
<http://www.fema.gov/about/stafact.shtm>

## **LESSON 11 TOPIC: CIPR 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 terrorism-based scenario. This scenario will consist of four modules (Pre-incident, Warning, Activation, Extended Response) in chronological order and portrays a series of conventional improvised explosive device (IED) attacks against critical infrastructure target sets across multiple sectors and regions of the United States. The TTX will address the 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. Learner discussion will focus on critical infrastructure protection 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:**

- Understand the various roles and responsibilities of government, the private sector, and the general public in the context of an emergent terrorist threat as well as an incident in progress
- Become familiar with the critical infrastructure incident management nodes, coordinating structures, and the processes through which they interact as discussed in the National Response Framework and its CIKR Support Annex
- Understand effects upon anticipated critical infrastructure sector actions resulting from changes in the national threat level through the National Terrorism Advisory System (NTAS)
- Understand the short and long-term impacts on the critical infrastructure sectors resulting from changes in the national threat level
- Become familiar with and assess public-private sector information sharing and intelligence in the context of incident management
- Become familiar with the processes and mechanisms used to build critical infrastructure situational awareness and facilitate public-private prevention, protection, 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?
- What are the key government and private sector incident management nodes and coordinating structures according to the NIPP and the National Response Framework?
- How are information and intelligence shared between the various public and private sector nodes of the NIPP Partnership Framework in an emergent threat scenario? Does the process work?
- How does the recent change from the Homeland Security Advisory System

(HSAS) to the NTAS affect critical infrastructure-related incident response? What actions do the sectors take in response to a national level NTAS elevation? What are the near and long-term ramifications across the sectors?

- How is situational awareness maintained among the various NIPP partners during incident response?
- How are private sector requests for assistance assessed and addressed during incident response operations?

### **3. Required Reading:**

National Infrastructure Advisory Council, *Framework for Dealing with Disasters and Related Interdependencies*, July 2009,

[http://www.dhs.gov/xlibrary/assets/niac/niac\\_framework\\_dealing\\_with\\_disasters.pdf](http://www.dhs.gov/xlibrary/assets/niac/niac_framework_dealing_with_disasters.pdf).

IS 800. *National Response Framework: An Introduction*, 2008,

<http://www.training.fema.gov/EMIWeb/IS/IS800b.asp>.

IS 821, *Critical Infrastructure Key Resource Support Annex*, 2008,

<http://training.fema.gov/EMIWeb/IS/IS821.asp>.

### **4. Additional Recommended Reading**

*National Incident Management System*, 2008,

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

## **LESSON 12 TOPIC: CIPR 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 table top exercise (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 protection 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:**

- Understand the various roles and responsibilities of government, the private sector, and the general public in the context of an emergent threat as well as an incident in progress
- Become familiar with the critical infrastructure incident management nodes, coordinating structures, and the processes through which they interact as discussed in the National Response Framework and its CIKR Support Annex
- Understand anticipated critical infrastructure sector actions resulting as a hurricane begins to be tracked offshore, approaches the U.S., makes landfall, and various response and recovery actions ensue
- Understand the short, medium, and long term impacts on the critical infrastructure sectors resulting from a catastrophic natural disaster
- Become familiar with and assess public-private sector information sharing products, processes, and systems used to support incident management operations
- Become familiar with the processes and mechanisms used to build critical infrastructure situational awareness and facilitate public-private prevention, protection, response, and recovery activities during naturally occurring incidents

### **2. Discussion Topics:**

- What are the roles and responsibilities of the various NIPP partners vis-à-vis national incident management? Differences from Exercise #1?
- What are the key government and private sector incident management nodes according to the NIPP and the National Response Framework?
- How is information pertinent to natural disaster preparedness and response shared between the various public and private sector nodes of the NIPP Partnership Framework in an emergent threat scenario? Is the process effective? How does it differ from what we saw in Exercise#1?
- What actions do the sectors take in response to the various phases of a catastrophic disaster lifecycle? What are the near, medium, and long-term ramifications across

- the sectors? Differences from Exercise #1?
- How is situational awareness maintained among the various NIPP partners during incident response?
  - How are private sector requests for assistance assessed and addressed during incident response operations?

### **3. Required Reading:**

National Infrastructure Advisory Council, *Framework for Dealing with Disasters and Related Interdependencies*, July 2009,  
[http://www.dhs.gov/xlibrary/assets/niac/niac\\_framework\\_dealingwithdisasters\\_slides.pdf](http://www.dhs.gov/xlibrary/assets/niac/niac_framework_dealingwithdisasters_slides.pdf)

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

NIST Technical Note 1476, Performance of Physical Structures in Hurricane Katrina and Hurricane Rita: A Reconnaissance Report,  
<http://www.tisp.org/index.cfm?pn=3&&pid=10261>.

IS 800, *National Response Framework: An Introduction*, 2008,  
<http://www.training.fema.gov/EMIWeb/IS/IS800b.asp>.

IS 821, *Critical Infrastructure Key Resource Support Annex*, 2008,  
<http://training.fema.gov/EMIWeb/IS/IS821.asp>.

### **4. Additional Recommended Reading**

*National Incident Management System*, 2008,  
[http://www.fema.gov/pdf/emergency/nims/NIMS\\_core.pdf](http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf).

**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 of the critical infrastructure protection 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 of the critical infrastructure protection 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 PROTECTION AND RESILIENCE RISK ENVIRONMENT**

**\*\*Special Activity: Collaborative Planning Project deliverable is due via e-mail on Lesson 15.**

**1. Lesson Goals/Objectives:**

- Develop an advanced understanding of potential future critical infrastructure operational and risk environments and related challenges
- Discuss the strategic choices that may impact our approach to critical infrastructure protection and resilience planning in the medium-long term future
- Discuss the types of planning efforts and investments that must begin to happen now to adequately prepare for the future world of critical infrastructure protection and resilience
- Review the complexities of critical infrastructure planning at the multi-jurisdictional, regional, and sector levels today and in the future
- Develop an advanced understanding of Federal, State, local, tribal, and private sector critical infrastructure protection and resilience requirements processes
- Understand the importance of critical infrastructure protection and resilience awareness, education, and training programs today and in the future

**2. Discussion Topics:**

- What will the critical infrastructure protection 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 will be the principal threats and challenges to critical infrastructure protection and resilience 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 protection and resilience be simulated and “wargamed” 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 things moving forward?
- What are the metrics that will guide relevant critical infrastructure protection and resilience feedback processes in the future?
- How are critical infrastructure protection 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 protection and resilience planning in the future? How can critical infrastructure protection 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 protection and resilience awareness, education, and training program?
  - What are the keys to effective critical infrastructure protection and resilience program management today and in the future?

### **3. Required Reading:**

Bob Prieto, *Infrastructure Resiliency: Do We Have the Focus Right?* November 16, 2009, <http://www.tisp.org/index.cfm?cdid=11838&pid=10261>.

Robert L. Reid, *The Infrastructure Crisis: Civil Engineering*, January 2008, <http://www.tisp.org/index.cfm?cdid=11036&pid=10261>.

Toffler Associates, *Guarding Our Future: Protecting our Nation's Infrastructure*, 2008, <http://www.toffler.com/docs/Guarding-Our-Future.pdf> /.

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

*National Infrastructure Protection Plan*, Chapters 6&7; Appendix 6. [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

**ATTACHMENT 1**  
**CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE INCIDENT**  
**MANAGEMENT EXERCISE #1**  
**TERRORISM SCENARIO**

**MODULE 1: PRE-INCIDENT**

**1. Scenario Build**

- A new Al Qaeda video is released on several Arabic internet sites focused on attacks targeting European and American interests worldwide, with a particular emphasis on 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.
- 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 attacks within Europe (timing unspecified) and admits to planning a failed attack in Istanbul 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 downtown 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.
- 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 in Germany, Italy, and possibly elsewhere in the final stages of operational planning and mission rehearsal.

- 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.

### **3. Discussion Questions**

- What actions would German authorities be taking in response to the attack? Italian authorities? Other European countries?
- What information would German authorities be sharing with U.S. government counterparts at this time?
- 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 “white noise” from a U.S. perspective?
- Would there be any changes recommended to protective measures across the critical infrastructure sectors based on 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 would the various key nodes of the NIPP incident management framework 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 an unspecified “WMD” capability.

- Several major news agencies receive phone calls from unidentified sources warning of an impending “reign of terror” 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 conduct national conference calls and provide briefings on the threat to critical infrastructure sector partners.
- The U.S. national threat level is increased to “elevated,” through the NTAS with specific emphasis on commercial facilities, national monuments, government facilities, and the transportation sector (highways, rail, mass transit, ferries, and ports), as well as for the geographical areas of the National Capital Region and New York State Region.

## 2. Discussion Questions

- What are your major personal and organizational concerns at this point?
- Would there be any intelligence updates to the private sector or State and local government officials at this time? If so, how would this process work?
- What are the essential elements of intelligence and related information required by your jurisdiction, agency, community, industry?
- What preventive/protective measures would government and the private sector put in place at this point? How would they be communicated to one another?
- What recommendations would these entities make regarding the NTAS threat level? 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 incident management framework be engaged in at this point?
- How would the NIPP partnership act to better understand the nature of and take action to mitigate the unspecified “WMD” threat? Are critical infrastructure owners/operators and mass public venue security officials prepared to deal with chemical and other potential WMD threats?

## MODULE 3: ACTIVATION

### 1. Scenario Build

- **Today 8:32 a.m. EDT**
  - Two large rental trucks drive into the Ft. Pitt and Squirrel Hill tunnels 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**
  - An 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**
  - An 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**
  - In Chicago, a minivan is detained in front of Chicago's O'Hare Airport for loitering in the Passenger Drop-off Zone. Upon investigation, the minivan is found to be carrying ten unidentified "chemical" canisters packed with homemade explosive. The driver is taken into custody and held at a local FBI detainment facility. O'Hare Airport remains open to the public, although under heightened security conditions.
  
- **9:18 a.m. EDT**
  - In Indianapolis, two bombs explode in the vicinity of the Soldiers' and Sailors' monument. Six people are injured in the blast. There are no fatalities. Local law enforcement authorities and the FBI are investigating surveillance camera video of the area. The immediate area around the monument has been closed to the public and traffic has been rerouted pending further investigation.
  
- **10:00 a.m. EDT**
  - The NTAS national threat level is elevated to "imminent" for airports, tunnels and bridges, mass transit, commercial facilities, government facilities and national monuments and icons. All other sectors remain at an "elevated" level under the NTAS.
  
- **12:00 a.m. EDT**
  - 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. Every city of evil will be touched; the child

of every criminal will know fear and death as our children have known it.”

## **2. Discussion Questions**

- What are your principal concerns and priorities at this time?
- How does the “WMD Factor” complicate emergency protection and response activities?
- What types of intelligence updates would be provided at this time, to whom, and by whom?
- 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 National Response Framework are operational at this point?
- What actions are being undertaken by the sector operations centers, ISACs or other information sharing entities?
- 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**

### **1. Scenario Build**

- **Two weeks from the Attacks in the United States**
  - DHS releases a statement from the Secretary lowering the NTAS threat level but maintaining a level of “elevated” for government facilities, commercial facilities, national monuments, and the transportation sector (highways, rail, ferries, mass transit, ports and airports).
  - The FBI announces that they have arrested three men associated with the 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.
  - The national and international impacts of the terrorist attacks in the United States have been extraordinarily high, cascading across the sectors domestically and internationally. The stock market has fallen to recession levels, with downward trends globally.
  - State and local officials have severely taxed their local first responder communities over the course of the period of heightened alert following

the attacks. Private sector security and emergency response forces have been similarly stressed. The costs of a “new threshold for security” are being felt to varying degrees across the sectors.

- 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 attack remains high.
- **Three weeks from the attacks in the United States**
  - DHS releases a statement from the Secretary lowering the national threat level for all sectors.
  - Pipe bombs are found at a high school in Chicago, Illinois. Two students are arrested.
  - 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.

## **2. Discussion Questions**

- What are your principal concerns in this phase of incident management?
- What types of enhanced prevention and protection activities would you be continuing 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 threat level had on your organization/constituency?
- What is the “new normal” for your agency, jurisdiction, corporation, 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?
- 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 30<sup>th</sup> 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, and tribal 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 protection and resilience public 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 protection 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 1<sup>st</sup>, 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 2<sup>nd</sup>. By the early morning hours of September 4<sup>th</sup>, 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 7<sup>th</sup>, with sustained winds of more than 120mph and entered the Gulf of Mexico on September 9<sup>th</sup> 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 protection and resilience public 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 protection 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 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 protection 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 9<sup>th</sup> through the 12<sup>th</sup>, 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 14<sup>th</sup>.
- Widespread storm surge flooding occurred in Southeast Louisiana, with Federal protection levees overtopping in the metro New Orleans area, producing pockets of significant flooding in low lying areas along the Mississippi River. In addition, Heidi produced 8-10 inches of rainfall which aggravated the storm surge flooding and brought many of the major rivers north of Lake Pontchartrain into flood stage. Although Heidi weakened upon moving inland, strong winds and torrential rains make movement impossible even in areas that were not inundated by flood waters.
- Presidential disaster declarations are made for the impacted counties in TX and LA. Federal incident coordination structures and field offices are activated.
- Over 2.5 million people are displaced from the region running from Northeast Texas to New Orleans. Additionally, the following major infrastructure damages/disruptions are noted:
  - Over 4M customers are without power in the region, to include numerous major hospitals and special needs facilities
  - Numerous major transformer towers are down in SW Louisiana
  - Major rail and highway networks are shut down and/or damaged
  - The I-10 bridge across Lake Pontchartrain has been dismembered in several places; other secondary and tertiary bridges are down throughout the region
  - Two major nuclear power plants in the region have suffered minor damages, but have been placed in shut down mode
  - Over a dozen major oil and natural gas pipelines are inoperative, with extent of damages unknown
  - More than one hundred Gulf oil platforms have been evacuated; several are now “free-floating”
  - Six major oil refineries in the region have been extensively damaged and will require long repair times
  - Cellular communications have been significantly degraded throughout the region; cell towers are down across the area
  - Dozens of major chemical plants and hazmat facilities are under 4-8 feet of

water; numerous chlorine rail tankers are overturned on site throughout the area

- The Mississippi River channel is blocked by floating debris and sunken vessels in numerous locations south of New Orleans and is temporarily closed to commercial traffic; major petroleum and agricultural import/export operations have been suspended
- Gasoline is in short supply across the region; first responder operations have priority
- Minor civil disorder and looting activities are reported in several cities and towns in the impacted area

## **2. Discussion Questions**

- What are the principal concerns of the agency/organization that you represent at this stage? What are your information sharing requirements at this stage? How are you getting the information you need?
- How do the various critical infrastructure protection and resilience public and private sector partners coordinate with each other and maintain a common situational awareness following hurricane landfall? What form does this coordination take? How does the agency/organization that you represent fit into this scheme?
- What types of analytical products, imagery, damage assessment products/services are available to help guide critical infrastructure protection 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 protection 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?
- 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 15<sup>th</sup>, 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 17<sup>th</sup>, 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 protection 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/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?
- Does the NIPP framework adequately address long term recovery issues?
- What are the major takeaways that you have from this exercise?