

**Course Number: XXXX**

**Course: Introduction to Critical Infrastructure Protection and Resilience**

**University of XXXXXX**

**Fall/Spring Semester 20XX**

**NAME OF SCHOOL:**

**DEPARTMENT:**

**PROGRAM:**

**PROFESSOR:**

Telephone Number:

Office Location:

Office Hours:

Email:

Website:

**COURSE DESCRIPTION/OVERVIEW:**

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, hazardous materials spills, industrial accidents, pandemic influenza, and cyber intrusions, among various others. Within this risk environment, our critical infrastructures are inherently vulnerable — domestically and internationally — 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 appropriately balancing resilience — a traditional American strength — with risk-based prevention, protection, and preparedness activities so that we can manage and reduce the most serious risks to the American people and the infrastructures that serve them. Putting this strategy into practice, in turn, requires an unprecedented partnership between the public and private sectors at all levels.

This 15-lesson graduate level course provides an introduction to the policy, strategy, and practical application of critical infrastructure protection and resilience from an all-hazards perspective. It describes the strategic context presented by the 21<sup>st</sup> century risk environment, and discusses the challenges and opportunities associated with the following: infrastructure- related public-private partnerships; information-sharing; risk analysis and prioritization; risk mitigation; performance metrics; program management; incident management; and investing for the future.

This is a multi-faceted course that will expose participants to complex intergovernmental

and public-private sector policymaking; risk analysis and management; strategic planning; and crisis management. The course is designed to promote subject-matter understanding, critical analysis of issues, and insight into senior leader decision-making. It also includes a practical examination of stakeholder interaction and key subject-matter areas through an interactive tabletop exercise, research paper, and oral presentation. The course promotes a holistic understanding of various approaches to critical infrastructure protection and resilience, applicable to the 18 sectors identified in the National Infrastructure Protection Plan, as well as infrastructure which crosses national borders or is inherently international.

**CREDITS CONFERRED: 3**

**PREREQUISITE:** None

**LEARNER OUTCOMES/OBJECTIVES (AS MAPPED AGAINST DEPARTMENT OF HOMELAND SECURITY CRITICAL INFRASTRUCTURE CORE COMPETENCIES):**

This course is designed to enable learners to:

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

- The history of critical infrastructure protection and resilience as a policy area, overarching policy approaches, and implications for policy making today
- Specific evolution of critical infrastructure protection and resilience as a national policy focus area under the Clinton, Bush, and Obama Administrations
- Congressional engagement in the critical infrastructure protection and resilience policy area post 9-11 and post-Katrina
- 9-11 attacks and Hurricane Katrina as focusing events

**2. Demonstrate an understanding of the 21<sup>st</sup> century risk environment as it applies to the critical infrastructure protection and resilience mission area:**

- Threats: Terrorism, cyber attacks, natural disasters and naturally occurring phenomena, industrial accidents and other manmade events, and other emergencies
- Vulnerabilities (facility, node, and system level)
- Consequences (public health and safety, economic loss/disruption, continuity of government and essential services, iconic loss, etc.)
- Dependencies/interdependencies
- Informing executive and managerial decision-making that can reduce risk and increase resilience for the Nation

**3. Be able to discuss the requirements and implications of the authorities, roles, responsibilities, and capacities of key critical infrastructure protection and resilience public and private sector stakeholders:**

- Federal, State, tribal, territorial, local, regional, private sector, and international
- Private sector issues and concerns
- Regulations, incentives, and motivations

**4. Examine critical infrastructure protection and resilience partnership frameworks, information sharing processes and systems, and coordination/collaboration challenges:**

- Federal, State, tribal, territorial, local, regional, private sector, and international collaboration, coordination, and communication
- Critical infrastructure data collection, warehousing, and protection
- Systems challenges and opportunities

**5. Analyze different strategic approaches and issues regarding critical infrastructure risk analysis, risk mitigation, and performance measurement (regulatory and non-regulatory):**

- Physical security
- Cybersecurity
- Insider threats
- Resilience
- Systems dependencies/interdependencies
- Regional partnerships
- Sector approaches

**6. Demonstrate an understanding of the critical infrastructure protection and resilience risk analysis and management framework as currently applied within and across the various Critical Infrastructure Sectors:**

- 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

**7. Demonstrate an understanding of the multi-faceted critical infrastructure protection and resilience partnership in action: national critical infrastructure protection and resilience incident management framework, selected case studies, and in-class exercises:**

- 9/11
- National Terrorism Advisory System (NTAS) Elevations
- Madrid/London Transit Bombings
- Hurricane Katrina
- California Wildfires
- Mumbai
- Deep Water Point Oil Spill
- Cyber Threats and Incidents

**8. Demonstrate an understanding of the complexities associated with effective and efficient critical infrastructure protection and resilience program management in a dynamic risk and future operating environment:**

- Developing sector-specific, jurisdictionally-based or regionally-focused critical infrastructure protection and resilience goals, objectives, risk mitigation approaches, and plans
- Designing and applying continuous feedback mechanism to measure critical infrastructure protection and resilience program performance
- Designing and implementing critical infrastructure protection and resilience awareness, education, and training plans and programs
- Doing more with less: critical infrastructure protection and resilience in a resource constrained environment
- Planning for the future risk and critical infrastructure operational environments

**DELIVERY METHOD:**

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, and 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.). Participants are expected to familiarize themselves with the assigned topics and readings before class and should be prepared to discuss and debate them critically as well as analyze them for biases and multiple perspectives.

**GENERAL COURSE REQUIREMENTS:**

1. Class attendance is both important and required. If, due to an emergency, you will not be in class, you must contact your instructor via phone or email. Learners with more than two absences may drop a letter grade or lose course credit.
2. It is expected that assignments will be turned in on time (the beginning of the class

in which they are due). However, it is recognized that learners occasionally have serious problems that prevent work completion. If such a dilemma arises, please speak to the instructor in a timely fashion.

3. The completion of all readings assigned for the course is assumed. Since class will be structured around discussion and small group activities, it is critical for you to keep up with the readings and to participate in class.
4. All beepers and cell phones should be turned off before class begins.

### **GRADING:**

Class Participation	30%
Research Paper	30%
Research Paper Presentation	25%
Incident Management Exercise (Player Roles and Responsibilities Paper)	15%

### **ACTIVITIES, EXERCISE, AND RESEARCH PROJECTS:**

#### **1. Research Paper/Oral Presentation (55%)**

Each learner will prepare a 12-15 page research paper on a critical infrastructure protection and resilience issue of their choice (national, regional, state, local, territorial, tribal, sector, or international focus). The paper should be completed using the following organizational format: problem statement, background (include key players, authorities, resources, etc.), discussion (presentation of alternatives with the identification of pros and cons for each alternative), and recommendations (including rationale behind their selection). Footnotes and citations, if any, should be included on a separate sheet of paper in the proper format for review. The paper should focus on the benefits, drawbacks, and obstacles to the practical application of proposed policy alternatives. The recommendations section should clearly describe the rationale for the policy option of choice. Example research paper topics include the following:

- How to promote critical infrastructure resilience strategies and practices
- How to promote critical infrastructure information sharing among the National Infrastructure Protection Plan (NIPP) partners
- How to measure the performance of critical infrastructure protection and resilience programs within and across sectors and jurisdictions

As an alternative to a research paper, learners may submit a 12-15 page, section-by-section critique of an existing critical infrastructure protection and resilience sector or sub-sector level plan; critical infrastructure protection and resilience regional, State or municipal-level critical infrastructure protection and resilience plan; or Federal-level critical infrastructure protection and resilience plan or policy. Learner critiques should include alternative visions/strategies for successful critical infrastructure protection and

resilience program implementation within the sector, jurisdiction, or geographic region under study.

Each learner will present his/her research topic or critical analysis (no more than 25-30 minutes in length) to the class during Lessons 13-14. The presentation format will mirror that of the research paper. **Research papers will be submitted prior to class on Lesson 15. Papers may be submitted electronically.**

Prior approval of the topic for the research paper is required. **Learners should submit a one-paragraph written description of their proposed topic in class or via email for approval no later than the beginning of class on Lesson 5.**

## **2. Incident Management Exercise (15%)**

Learners will participate in a role-based, interactive tabletop exercise simulating 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**. Each learner will be assigned a role as a key public or private sector official with attendant critical infrastructure concerns and responsibilities. The exercise will include an emerging threat phase, operational response phase, and post-incident recovery phase. In preparation for the exercise, each participant will develop a short 2-3 page paper in 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 the classroom exercise.**

## **3. Expectations for Participation (30%):**

Participation includes coming to class prepared, participating in class discussion, and dynamic role playing during the critical infrastructure protection and resilience incident management exercise.

### **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 are identified as primary textbook readings for the course. These textbooks will be supplemented by additional readings accessible on-line, with website addresses provided in the lesson description section that follows below.

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

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

Brown, Kathi Ann. *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*, Spectrum Publishing Group, 2006.

**ARTICLES AND REPORTS:**

Various articles and reports are included as required and recommended readings within each individual lesson as described below.

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

## COURSE OUTLINE

### **LESSON 1 TOPIC: INTRODUCTION TO CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE**

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

- Become familiar with the scope of the course, administrative requirements, instructional methodology, evaluation criteria, and feedback processes
- Understand the evolution of critical infrastructure protection and resilience as a national policy focus area
- Become familiar with the various statutes and Presidential policy documents governing the application of critical infrastructure protection and resilience in the United States.
- Understand how critical infrastructure protection and resilience policy has changed as a function of the all-hazards risk environment, including specific threats and hazards
- Understand why the definition of critical infrastructure and the scope of the critical infrastructure protection and resilience sector construct have changed over time
- Understand the general critical infrastructure operational landscape across the sectors and the U.S. regionally

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

- What are critical infrastructures and why are they important to us?
- Why does critical infrastructure protection and resilience represent such a challenge?
- How has the critical infrastructure protection and resilience mission changed over time from a historical perspective?
- What are the general principles we typically associate with critical infrastructure protection and resilience in the U.S. context?
- How has the Nation's approach to critical infrastructure protection and resilience changed over time with regard to certain threats/hazards?
- How would you characterize critical infrastructure protection and resilience as a policy area prior to the Clinton Administration?
- What are the differences between and 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 and 2.

Collins and Baggett, Chapters 1-3.

Brown, Chapters 1-4, 8 and 9.

John D. Moteff. *Critical Infrastructure Protection: Background, Policy and Implementation*. 2008. <http://www.fas.org/sgp/crs/homsec/RL30153.pdf>.

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.fas.org/sgp/library/pccip.pdf>.

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*. 2009. Executive Summary, Chapters 1 and 5. [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:**

*The 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).

Clark Staten. *Reflections on the 1997 Commission on Critical Infrastructure Protection Report*. 1997. <http://www.blythe.org/nytransfer-subs/97cov/PCCIP; Critical Infrastructure Protection Report>.

**LESSON 2 TOPIC: EXAMINING CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE IN THE CONTEXT OF THE 21<sup>ST</sup> CENTURY RISK ENVIRONMENT**

**1. Lesson Goals/Objectives:**

- Understand the various threats that may impact critical infrastructure in the different sectors, and how they can be viewed in an all-hazards risk management approach
- Understand the evolving nature of the terrorist threat as it applies to critical infrastructure protection and resilience
- 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 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 do our critical infrastructure “target sets” play in the concept of “asymmetric warfare?”
- How have these threats evolved over time?
- Why do traditional critical infrastructures represent such preferred targets for malicious actors (international terrorists, domestic terrorists, criminal organizations, etc.)?
- Why would government expand its view of critical infrastructure to encompass targets that have amplifying effects, such as commercial facilities and monuments and icons?
- What are the principal challenges we face in ensuring the protection and resilience of our critical infrastructures in light of these threats?
- 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?
- What obstacles seem to hinder improvements to critical infrastructure protection and resilience?

**3. Required Reading:**

Brown, Chapter 5.

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://assets.opencrs.com/rpts/R41004\\_20100318.pdf](http://assets.opencrs.com/rpts/R41004_20100318.pdf).

Congressional Research Service Report, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*. 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.dtic.mil/cgi-bin/GetTRDoc?AD=ADA476034&Location=U2&doc=GetTRDoc.pdf>.

Rand Corporation. *The Lessons of Mumbai*. 2008. [http://www.rand.org/pubs/occasional\\_papers/2009/RAND\\_OP249.pdf](http://www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf).

*Mumbai Terrorist Attacks*. 2008. <http://www.mahalo.com/mumbai-terrorist-attacks>.

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).

Libicki, Chalk and Sisson. *Exploring Terrorist Targeting Preferences*. 2007. [http://www.rand.org/pubs/monographs/2007/RAND\\_MG483.pdf](http://www.rand.org/pubs/monographs/2007/RAND_MG483.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 3 TOPIC: EXAMINING CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE AUTHORITIES, ROLES, AND RESPONSIBILITIES: FEDERAL, STATE, TRIBAL, TERRITORIAL, LOCAL, AND PRIVATE SECTOR**

**\*\*Special Activity: Incident management exercise roles assigned by Instructor/Professor**

**1. Lesson Goals/Objectives:**

- Understand the various roles and responsibilities of government (Federal, State, tribal, territorial, local, and other nation's governments) and the private sector regarding critical infrastructure protection and resilience
- Understand the differences between regulated and voluntary critical infrastructure protection and resilience regimes across the critical sectors
- Understand the roles that nongovernmental organizations, the scientific/technology community, and academia play in critical infrastructure protection and resilience
- Understand the principal authorities and capacities regarding critical infrastructure protection and resilience across government and industry
- Understand 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?
- What are the key roles and responsibilities of the following with respect to critical infrastructure protection and resilience: Federal, State, tribal, territorial, and local governments; industry; academia; Research & Development entities; and nongovernmental organizations?
- How is each of the above players advantaged/disadvantaged regarding their individual critical infrastructure protection and resilience 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 the critical infrastructure protection and resilience mission?
- How does the distributed structure of critical infrastructure protection and resilience responsibility and accountability play out against the principal threats we face in this mission area?

**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 and 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.bhs.idaho.gov/Pages/FinanceAndLogistics/Grants/PDF/SRLTT%20Guide\\_fi\\_nal%20508%209-2008.pdf](http://www.bhs.idaho.gov/Pages/FinanceAndLogistics/Grants/PDF/SRLTT%20Guide_fi_nal%20508%209-2008.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>.

General Accounting Office, *Combating Terrorism: Intergovernmental Partnership in a National Strategy to Enhance State and Local Preparedness*, 2002, <http://www.gao.gov/new.items/d02547t.pdf>.

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

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 4 TOPIC: ORGANIZING AND PARTNERING FOR CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE AND NETWORKING TO SHARE INFORMATION**

**1. Lesson Goals/Objectives:**

- Understand the structures, processes, and coordinating mechanisms associated with the NIPP Partnership Model
- Understand the roles and responsibilities of the nature of collaborative interaction among the Sector Coordinating Councils, Government Coordinating Councils, and Regional Consortium Coordinating Councils
- Understand the various methods, processes, and systems that the various critical infrastructure protection and resilience partners use to share information with one another
- Become familiar with the ongoing challenges and barriers to information sharing and collaboration that exist among the various levels of government and the private sector
- Understand how critical infrastructure protection and resilience-related information is collected, warehoused, protected, and exchanged among various levels of government and the private sector

**2. Discussion Topics:**

- What are the key elements of the NIPP partnership model? What is the Critical Infrastructure Partnership Advisory Council (CIPAC)?
- 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 are the principal barriers to sharing information proactively and comprehensively between government and industry at all levels of the NIPP partnership?
- 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 the U.S. Department of Homeland Security (DHS); the Federal Bureau of Investigation (FBI); and the State, local and regional fusion centers regarding critical infrastructure protection and resilience information sharing and analysis?

- How are critical infrastructure protection and resilience information and intelligence that originate from multiple distributed sources compiled and deconflicted? Are we successfully “connecting the dots” today?
- How has real-world successes/failures led to improvements in information sharing among government and industry partners?

### **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 and 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).

*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://www.surfacetransportationisac.org/SupDocs/Library/ISAC\\_Products/isac\\_role\\_in\\_cip.pdf](http://www.surfacetransportationisac.org/SupDocs/Library/ISAC_Products/isac_role_in_cip.pdf).

*A Functional Model for Critical Infrastructure Information Sharing and Analysis*, 2004,  
[http://www.isaccouncil.org/index.php?option=com\\_docman&task=doc\\_view&gid=9&Itemid=208](http://www.isaccouncil.org/index.php?option=com_docman&task=doc_view&gid=9&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).

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>

### **4. Recommend Additional Reading:**

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

**LESSON 5 TOPIC: ASSESSING CRITICAL INFRASTRUCTURE RISK IN AN INTERDEPENDENT WORLD**

**\*\*Special Activity: Research paper topics must be submitted prior to class**

**1. Lesson Goals/Objectives:**

- Understand the major elements of risk in the context of critical infrastructure protection and resilience: threats, vulnerabilities, and consequences
- Understand how critical infrastructure protection and resilience-focused risk differ from that applied in the context of other disciplines (security, engineering, finance, and business)?
- Understand how the elements of risk relate to the human, physical, and cyber aspects of critical infrastructure protection and resilience
- Understand how terrorism risk differs from the risk represented by natural disasters and other manmade hazards
- Understand the DHS strategic risk assessment process, as well as how other government and private sector critical infrastructure protection and resilience stakeholders view and evaluate risk
- Understand the complexities regarding critical infrastructure dependencies and interdependencies as they relate to risk and its components
- Be familiar with how risk drives (or does not drive) risk management strategies 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 and its component elements? How are risks prioritized within the NIPP framework?
- How do the human, physical, and cyber dimensions of critical infrastructure protection and resilience relate to the concept of risk?
- Does terrorism risk differ from the risk associated with natural disasters and other manmade hazards? If so, how?
- How does the Federal government assess risk and communicate the results of the risk assessment process to other critical infrastructure protection and resilience 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 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 these dependencies and interdependencies?

- Can we ever get to a completely 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?

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

George Mason University, *Critical Infrastructure Protection: Elements of Risk*.  
 Various articles, 2007,  
[http://www.steelcityre.com/documents/RiskMonograph\\_1207.pdf](http://www.steelcityre.com/documents/RiskMonograph_1207.pdf).

U.S. Government Accountability Office, *Homeland Security: DHS Risk-based Grant Methodology is Reasonable, but Current Version's Measure of Vulnerability is Limited*,"  
 2008, <http://www.gao.gov/new.items/d08852.pdf>.

U.S. Government Accountability Office, *Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security*, 2008,  
<http://www.gao.gov/new.items/d08904t.pdf>.

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>.

**LESSON 6 TOPIC: ENABLING PROTECTION, MANAGING RISK, AND MEASURING PERFORMANCE: THE VOLUNTARY APPROACH**

**\*\*Special Activity: Learners will read and be prepared to discuss and provide examples related to one of the above sector plans in detail in class.**

**1. Lesson Goals/Objectives:**

- Identify those sectors in which security is a function of public-private sector voluntary collaboration and coordination
- Understand 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
- Become familiar with 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)
- Be familiar with the various resources made available by the Federal government to other levels of government and the private sector to foster critical infrastructure protection and resilience program development and implementation

**2. Discussion Topics:**

- What are the sectors in which security is not under government regulatory oversight? Which sectors use a hybrid voluntary-regulatory approach?
- 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 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?
- Is there one or more models 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 the next step(s) that this program needs to take to be successful?
- What are the various resources made available by the Federal government to other levels of government and the private sector to foster critical infrastructure protection and resilience program development and implementation?

### **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*, Chapter 3 & Appendix 3, 2009, <http://www.fas.org/sgp/crs/terror/RS21131.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>.

General Accounting Office, *Passenger and Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts*, 2007, <http://www.gao.gov/new.items/d07583t.pdf>.

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/publication/3275/mass\\_transit\\_security\\_after\\_the\\_london\\_bombings.html?breadcrumb=%2Fexperts%2F812%2Fdaniel\\_b\\_prieto](http://belfercenter.ksg.harvard.edu/publication/3275/mass_transit_security_after_the_london_bombings.html?breadcrumb=%2Fexperts%2F812%2Fdaniel_b_prieto).

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>

### **4. 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).

**LESSON 7 TOPIC: ENABLING PROTECTION, MANAGING RISK, AND MEASURING PERFORMANCE: THE REGULATORY APPROACH**

**1. Lesson Goals/Objectives:**

- Identify those sectors in which security or other risks are addressed through government regulation
- Understand how risks are assessed and managed and how performance is evaluated in those sectors in which security or preparedness for and response to other hazards are 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 a regulated party in the context of critical infrastructure protection and resilience

**2. Discussion Topics:**

- What are the sectors in which security and other threat types are addressed in government regulations?
- What are the different approaches to 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 individual approaches/models?
- What are the strengths and weaknesses of a regulatory approach to critical infrastructure protection and resilience?
- Do one or more models of regulation stand out as more effective than the others? If so, why?
- How do regulatory regimes deal with “outside-the-fence” security and emergency response concerns as well as critical dependency/interdependency issues?
- Is regulation working to produce a measurable increase in security or emergency preparedness in those sectors in which regulation is operative?

**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, <http://www.nrc.gov/security.html>.

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://www.gpo.gov/fdsys/pkg/FR-2009-05-20/pdf/E9-11736.pdf>.

Holt and Andrew, *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/homsec/RL33347.pdf>.

Committee to Review the Department of Homeland Security's Approach to Risk Analysis; National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis*, 2010, [http://download.nap.edu/cart/deliver.cgi?record\\_id=12972](http://download.nap.edu/cart/deliver.cgi?record_id=12972).

**LESSON 8 TOPIC: CYBERSECURITY AND SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) VULNERABILITIES: IDENTIFYING AND MANAGING “NANOSECOND” RISK AND PERFORMANCE**

**1. Lesson Goals/Objectives:**

- Understand the “borderless” nature of the cyber threats and challenges that impact the world of critical infrastructure protection and resilience
- 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 SCADA systems vulnerabilities
- Understand how cyber risk is assessed and managed within the various critical infrastructure sectors, as well as how cyber risk mitigation performance is evaluated

**2. Discussion Topics:**

- What are the principal threats and challenges of cybersecurity as they pertain to critical infrastructure protection and resilience? Is this a “real and present danger?” Why or why not?
- How does the 2009 White House CyberSecurity Review Report 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 sectors address the issues of cyber and SCADA vulnerabilities? How do we avoid “shifting risk” in this arena and resolve vulnerabilities in a definitive way?
- 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?

**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/new.items/d081157t.pdf>.

U.S. Government Accountability Office, *Cybersecurity: 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*, <http://www.gao.gov/new.items/d04354.pdf>

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

David Watts, *Security and Vulnerability in Electric Power Systems*,  
<http://eric.purpletree.org/file/PaperECE723v39Format.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 9 TOPIC: THE INTERNATIONAL DIMENSION OF CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE**

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

- Understand the international dimensions of critical infrastructure protection and resilience as defined in the NIPP with a particular focus on supply chain dependencies/interdependencies
- Become familiar with various alternative approaches to critical infrastructure protection and resilience in use internationally
- Become familiar with various structures and forums that are used to promote international critical infrastructure protection and resilience cooperation and collaboration

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

- What does the NIPP have to say regarding the international dimension of critical infrastructure protection and resilience?
- Why do we need to press for critical infrastructure protection and resilience outside our own borders? Supply chain considerations? Who should be our principal international critical infrastructure protection and resilience partners? Why?
- What are the typical approaches to critical infrastructure protection and resilience used outside the United States? What are their strengths and weaknesses? Are these primarily regulation driven or is a voluntary approach used? Does a “model” critical infrastructure protection and resilience regulatory program exist abroad?
- Is there a structure(s) through which international critical infrastructure protection and resilience issues can be addressed?
- Is there a national, bi-national, or multi-national critical infrastructure protection and resilience program that stands out as a model or best practice?
- How should multi-lateral critical infrastructure protection and resilience cooperation and collaboration be incentivized?
- What should constitute the major elements of a U.S. international critical infrastructure protection and resilience strategy? How would such a strategy best be implemented and through what mechanism?

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

*National Infrastructure Protection Plan*, Appendix 1b.

Boin, Arjen, and Rhinhard, *Institutionalizing Homeland Security Cooperation in Europe*, 2007, [http://www.allacademic.com/meta/p\\_mla\\_apa\\_research\\_citation/2/5/0/8/6/pages250863/p250863-1.php](http://www.allacademic.com/meta/p_mla_apa_research_citation/2/5/0/8/6/pages250863/p250863-1.php).

NATO Parliamentary Assembly, *The Protection of Critical Infrastructures*, 2007 Annual Session, <http://www.Nato-pa.int/default.asp?CAT2=1159&CAT1=16&CAT0=2&com=1165&MOD=0&SMD=0&SSMD=0&STA=0&ID=0&PAR=0&PRINT=1>.

European Commission, *Protecting Europe from Large-scale Cyber attacks and*

*Disruptions: Enhancing Preparedness, Security and Resiliency*, 2009,  
[http://ec.europa.eu/information\\_society/policy/nis/docs/comm\\_ciip/comm\\_en.pdf](http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf).

Council of the European Union, *Council Directive 2008/114/EC: Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve their Protection*,  
<http://www.euractiv.com/en/security/critical-infrastructure/article-140597>.

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>.

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).

Critical Infrastructure Protection Website (Australia),  
[www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity\\_CriticalInfrastructureProtection](http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection)

## **LESSON 10 TOPIC: EMERGENT THEMES AND ISSUES**

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

- Become familiar with various emergent themes and issues in the critical infrastructure protection and resilience world
- Understand emergent threats and corresponding risk mitigation approaches
- Become familiar with current Federal critical infrastructure protection and community resilience-related resilience strategies and initiatives
- Become familiar with major efforts currently underway to develop and implement critical infrastructure protection and resilience strategies and initiatives at the State and local level, as well as across the private sector
- Understand the relationship between critical infrastructure resilience and community resilience

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

- What is the concept of “Resilience” as it applies to critical infrastructure protection and resilience?
- What are the general principles associated with resilience as currently applied within government and industry?
- What are the similarities and differences between “Critical Infrastructure Resilience” and “Community Resilience?” How does one impact the other?
- 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:**

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

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)

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>.

## **LESSON 11 TOPIC: MANAGING INCIDENTS IN AN ALL-HAZARDS ENVIRONMENT**

**\*\*Special Activity: Incident Management Exercise Preparation.** Today's class involves an informal walk-through of next lesson's interactive, discussion-based table top exercise (TTX) driven by a terrorism-based scenario. This lesson will focus on gaining an understanding of the National Incident Management System (NIMS) and the National Response Framework (NRF) as they apply to critical infrastructure protection and resilience in the context of incident management. This lesson will also explore the relationship between the NIPP and the NRF in detail, including an examination of how the public and private sectors share information, maintain situational awareness, and provide assistance to one another during all-hazards emergencies. This scenario will consist of four modules (Pre-incident, Warning, Activation, and 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 focus on the roles, responsibilities, and interaction between Federal, State, tribal, territorial, and local governments; 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 communication and information sharing, coordination, integration of capabilities, and problem identification and resolution.

### **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 protection and resilience key incident management nodes and the processes through which they interact as discussed in the NRF and its CIKR Support Annex
- Understand anticipated sector actions resulting from changes in the national threat level through the National Terrorism Advisory System (NTAS) or other means
- 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 situational awareness and facilitate public-private critical infrastructure-related 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 according to the NIPP and the NRF?
- 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?
- What actions do the sectors take in response to a national level NTAS elevation?

- How does this process work? 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\\_dealing\\_with\\_disasters.pdf](http://www.dhs.gov/xlibrary/assets/niac/niac_framework_dealing_with_disasters.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).

**LESSON 12 TOPIC: CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE  
INCIDENT MANAGEMENT EXERCISE (STUDENT ACTIVITY)**

**\*\*Special Activity: Incident Management Point papers 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, and 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 focus on the roles, responsibilities, and interaction between Federal, State, tribal, territorial, and local governments; 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 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 key incident management nodes and the processes through which they interact as discussed in the NRF and its CIKR Support Annex
- Understand anticipated sector actions resulting from changes in the national threat level through the NTAS or other means
- Understand the short and long term impacts on the 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 situational awareness and facilitate public-private critical infrastructure-related 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 according to the NIPP and the NRF?
- 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?
- What actions do the sectors take in response to a national level NTAS elevation? How does that process work? 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 according to the NRF CIKR Support Annex?

### **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 13 TOPIC: PRESENTATIONS (ACTIVITY)**

**1. Lesson Goals/Objectives:**

- Provide a critical analysis of a key critical infrastructure protection and resilience issue or a critical infrastructure protection and resilience-related plan or policy and provide recommendations for improvement

**2. Discussion Topics:**

- Presentations

**3. Required Reading:**

- As required for research paper and presentation

**LESSON 14 TOPIC: PRESENTATIONS (ACTIVITY)**

**1. Lesson Goals/Objectives:**

- Provide a critical analysis of a key critical infrastructure protection and resilience issue or critical infrastructure protection and resilience -related plan or policy and provide recommendations for improvement

**2. Discussion Topics:**

- Presentations

**3. Required Reading:**

- As required for research paper and presentation.

**LESSON 15 TOPIC: MANAGING AN EFFECTIVE CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE PROGRAM AND PREPARING FOR THE FUTURE RISK ENVIRONMENT**

**\*\*Special Activity: Final Research Papers are due via e-mail before class.**

**1. Lesson Goals/Objectives:**

- Become familiar with potential future critical infrastructure protection and resilience operational and risk environments and related challenges
- Become familiar with strategic choices that may impact our approach to critical infrastructure protection and resilience in the medium-long term future (10-20 years from now)
- Be familiar with the types of investments that must begin to happen now to adequately prepare for the future world of critical infrastructure protection and resilience
- Understand the complexities of critical infrastructure protection and resilience planning at the multi-jurisdictional, regional, and sector levels today and in the future
- Understand Federal, State, tribal, territorial, and local 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?
- 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 “war-gamed” today?
- What actions should we be taking now to buy down future risk and position the next generation for success in this area? Will today’s priorities set us up for success?
- 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 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:**

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>.

Toffler Associates, *Creating a Secure Future: Understanding and Addressing the Threat to TIH Rail Cargoes*, 2008, <http://www.toffler.com/docs/Creating-a-Secure-Future.pdf>.

Toffler Associates, *Protecting our Space Capabilities: Securing the Future*, 2008, <http://www.toffler.com/docs/Protecting%20Our%20Space%20Capabilities%20-%20Securing%20the%20Future%20080723v2.pdf>.

*National Infrastructure Protection Plan*, Chapters 6 and 7; Appendix 6, [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, (General review only) Office of Infrastructure Protection Strategic Plan: FY 2008-2013. <http://www.iaem.com/publications/News/documents/OfficeofInfrastructureProtectionStrategicPlanFY08-13.pdf>.

**ATTACHMENT 1**  
**CIPR INCIDENT MANAGEMENT EXERCISE**  
**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, and government centers. The video describes “striking the infidels where they are most vulnerable.”
- There is only a brief mention of the video in daily news reporting, and the general public is unaware of any threat.
- Officials in the United Kingdom 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 Rome 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 home bomb-making instructions has proliferated greatly in recent months.

**2. One Month Later**

- Victoria Station in London (London Tube), a major hub station for the city averaging over a million commuters daily, is attacked. A man carrying a backpack is apprehended by U.K. 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 U.K. detention facility for questioning after being treated for second-degree burns at a local hospital. A second bomb explodes on a crowded metro bus outside the Victoria Station. Twenty people are killed and three dozen more are wounded. The bomber was killed during the attack. It is believed that the two incidents are linked based upon preliminary analysis of video surveillance footage.
- 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 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 the United Kingdom and elsewhere in the final stages of operational planning and mission rehearsal.

- The Government of the United Kingdom has elevated security around governmental facilities, major transportation hubs, and other potential targets across the country. The London metro system remains open, but is operating under heightened security conditions.
- Although the national threat level has not been raised through the NTAS, special screening procedures are in place for flights inbound to the United States from the United Kingdom.

### **3. Discussion Questions**

- What actions would U.K. authorities be taking in response to the attack?
- What information would U.K. 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 U.S.?
- 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 the United Kingdom, the FBI and DHS have received increased reporting of multiple impending attacks on commercial facilities, national monuments, and the transportation sector (highways, rail, ferries, and ports) across the United States.
- Exact method 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 station Al Jazeera from an Al Qaeda affiliate with known operations in Europe and Southwest Asia claiming responsibility for the pending attacks on the United States.
- 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 and surface transportation and conduct national conference calls and provide briefings on the threat.

- The U.S. national threat level is increased to “elevated,” with a focus on commercial facilities, national monuments, 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. Special screening procedures remain in effect for all domestic and international flights.

## 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 this point? How would they be communicated to one another?
- What recommendations would these entities make regarding the national threat level through the NTAS? 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?

## MODULE 3: ACTIVATION

### 1. Scenario Build

- **Today 8:32 a.m. EDT**
  - Two large rental trucks drive into the Fort McHenry Tunnel on Interstate 95 and Baltimore Harbor Tunnel on Interstate 895 and explode. A large fire burns in the Fort McHenry Tunnel and there is a partial collapse of the Baltimore Harbor Tunnel. Both tunnels are closed. Fifty-five commuters are killed and over one hundred are injured.
- **8:50 a.m. EDT**
  - An IED is detonated in Washington, D.C.’s Union Station; six people are killed and thirty people are injured. Union Station has been closed to the public.
- **8:52 a.m. EDT**
  - An IED is found outside the main entrance of Philadelphia’s 30th Street Station. The IED is cordoned off and disarmed. The station is temporarily closed to the public while further bomb inspections are conducted.

- **10:04 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 propane 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.
- **10:08 a.m. EDT**
  - In St. Louis, two bombs explode in the vicinity of the St. Louis Arch. 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 Arch has been closed to the public until further notice.
- **10:30 a.m. EDT**
  - The national threat level is elevated to "severe" for airports, tunnels and bridges, mass transit, commercial facilities, government facilities, and national monuments and icons. All other sectors are raised to orange.
- **12:00 a.m. EDT**
  - Another internet video is released from an Al Qaeda affiliate taking credit 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?
- 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 NRF 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**
  - 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 London 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 except for aviation, which remains at “elevated.”
  - Pipe bombs are found at a high school in St Louis, MO. 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 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?