**Course Number: XXXX**

**Critical Infrastructure Security and Resilience Capstone Seminar**

**University of XXXXXX**

**Fall/Spring Semester 20XX**

**Name of School:**

**Department:**

**Professor:**

Telephone Number:

Office Location:

Office Hours:

Email:

Website:

**Course Description/Overview:**

Critical infrastructure security and resilience is an emerging multidisciplinary field with growing significance in the context of homeland security, public policy, risk management, business administration, and many others. It requires individuals to apply strategic, critical, and analytical processes that can adapt to rapidly changing technological, societal, and economic conditions addressed in the context of a 21st century risk environment characterized by 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 mitigations activities that allow us to manage the most serious risks.

This is a 15-lesson graduate-level capstone seminar intended to foster the development of an advanced baseline of relevant knowledge among seminar participants and apply this baseline to “hands-on” critical infrastructure security and resilience strategy and plan development through in-classroom case studies and incident management exercises. It targets graduate students in multiple disciplines and mid-career professionals looking to enhance their knowledge, critical thinking, and analytical skills needed to fulfill the roles and responsibilities related to critical infrastructure.

**Credits Conferred:** 3

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

**Course Goals/Objectives (As Mapped Against Department of Homeland Security Core Competencies):**

This course is designed to enable learners to:

**1. Analyze critical infrastructure security and resilience as a core homeland security policy area.**

**2. Evaluate the 21st century risk environment in the context of the critical infrastructure security and resilience mission.**

**3. Apply the building blocks of critical infrastructure security and resilience strategy development, planning, and incident management operations through selected case studies and in-class exercises.**

**Delivery Method/Course Requirements:**

Course delivery will be through mini-lectures, structured collaborative projects, case studies, exercises, guest speakers, and interactive classroom discussions. The assigned course readings include a variety of resources, such as legislation and policy documents, industry and external reviews, and academic articles. 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:**

Collaborative Planning Project 40%

Case Studies 30%

Incident Management Exercise 15%

Classroom Participation 15%

**Oral/written requirements:**

1. **Collaborative Planning Project/Oral Presentation (40%):**

Learners will work collaboratively in 3-4 person teams to develop a critical infrastructure security and resilience strategy, plan, or program targeted at the corporate (enterprise level), sector, jurisdictional (FSLTT), 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 security 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 30-40 minutes in length. **The completed written project deliverable is to** **be submitted at the beginning of class on the day of the oral presentation.**

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

1. **Case Studies (30%):**

Learners will apply critical infrastructure security and resilience knowledge and skills to three selected case studies. Prior to class, learners should read the specified case narrative and be prepared to engage in critical analysis. Subsequent to each in-class discussion and evaluation, learners will complete a 2-3 page reflection paper chronicling his/her experience and lessons learned. **Reflection papers will be submitted at the beginning of the next class.**

1. **Incident Management Exercise (15%):**

Learners will participate in an interactive tabletop exercise that simulates 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 student 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 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 the scheduled classroom exercise.** Individual roles for the exercise will be assigned by the instructor during class on **Lesson 4**.

1. **Expectations for Participation (15%):**

Participation includes coming to class prepared, engaging in class discussions, being a full partner in group activities and case studies, 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, 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 written products. 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, ed., *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Wiley-Interscience, 2006).

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

*Protection* (Praeger Security International, 2009).

**Grading Scale (School Policy Dependent):**

**Lesson 1 Topic: Understanding the Evolution of Critical Infrastructure Security and Resilience**

**1. Lesson Goal(s)/Objective(s)**:

* Review the course scope, administrative requirements, instructional methodology, evaluation criteria, and feedback processes.
* Explain the evolution of critical infrastructure security and resilience as a national policy focus area.

**2. Discussion Topics:**

* Why and how have the definition of “critical infrastructure” and the scope of the critical infrastructure security and resilience sector-focused construct changed over time?
* Define “security,” and “protection.”
	+ What are the similarities/differences?
* How is critical infrastructure currently categorized? What is the rationale? Benefits? Challenges in terms of grouping infrastructure into sectors?
* How have major events shaped or influenced public policy relating to critical infrastructure? Discuss the social, economic, and political factors driving critical infrastructure policy.
* How does public policy for critical infrastructure influence, impact, or reflect the realities faced by private industry?

**3. Required Reading**:

Collins and Baggett, *Homeland Security and Critical Infrastructure*

*Protection*, chaps. 1-3.

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

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

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

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

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

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

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

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

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

**Lesson 2 Topic: Analyzing Resilience**

**1. Lesson Goal(s)/Objective(s)**:

* Analyze the evolution and current understanding of “resilience” as it relates to critical infrastructure security.

**2. Discussion Topics**:

* 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 security and resilience planning?
* What are the similarities and differences between “critical infrastructure resilience” and “community resilience?”
* What are the various approaches to operationalize resilience at a regional and sub-regional level?
* What are the major recommendations of the 2009 National Infrastructure Advisory Council (NIAC) Report regarding resilience? Do you concur with them? If not, what would be your recommendations?
* Are our critical infrastructures more resilient in a post-Katrina world? The evolving world of the future?

**3. Required Reading**:

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

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

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

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

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

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

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

Post-Katrina Emergency Management Reform Act of 2006, S. Bill. No. S.3721 (2006) <https://beta.congress.gov/bill/109th-congress/senate-bill/3721/text>.

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

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

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

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)

**4. Recommended Additional Reading:**

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

U.S. 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>.

**Lesson 3 topic: Identifying Authorities, Roles, and Responsibilities**

**1. Lesson Goal(s)/Objective(s)**:

* Evaluate the political, organizational, legal, and resource challenges faced by critical infrastructure security and resilience stakeholders in executing their responsibilities.

**2. Discussion Topics**:

* Who is “in charge” of critical infrastructure security and resilience nationally, regionally, locally, and across the 16 critical sectors? How is planning structured/conducted at each jurisdictional level? Between the public and private sectors horizontally?
* What are the key authorities, roles, responsibilities, and capacities of the following with respect to critical infrastructure security and resilience?
	+ FSLTT; industry; academia; Research and Development (R&D) entities; and nongovernmental organizations?
* How are each of the above players advantaged/disadvantaged regarding their individual critical infrastructure security and resilience planning roles and responsibilities?
* How do the various government and private entities with critical infrastructure security and resilience responsibilities at different levels interact and collaborate with one another?
* How are the 16 critical infrastructure sectors organized to accomplish the critical infrastructure mission at the sector and sub-sector level? What is their “motivation” regarding their roles 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?
* How are high impact, low frequency threats addressed in the NIPP framework? Across sectors? Within industry?
* Does our national policy and planning framework effectively and efficiently enable critical infrastructure security and resilience planning and program implementation at the regional level? State level? Local level? Corporate level? Cite examples from your own experience.

**3. Required Reading**:

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

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

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

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

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

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

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

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

**Lesson 4 Topic: Examining Critical Infrastructure Sector Approaches**

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

**\*\*Special Activity: Collaborative Planning Project focus area description due to Instructor/Professor**

**1. Lesson Goal(s)/Objective(s)**:

* Assess the strengths and weaknesses of regulated and voluntary critical infrastructure security and resilience approaches.

**2. Discussion Topics**:

* What are the different approaches to security regulation across the sectors? How does each address the major areas of risk assessment, management, and performance measurement?
* How do the regulators and regulated parties relate to one another in these different approaches/models?
* Is there one or model of regulation and/or voluntary security collaboration/coordination that stands out as more effective than the others? If so, why?
* How do regulatory and voluntary regimes deal with “outside-the-fence” security concerns as well as critical dependency/interdependency issues?
* How do these approaches impact the planning and performance measurement processes?
* Why have other industrialized countries avoided a regulatory regime for some sectors that the United States regulates?
* 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, *Homeland Security and Critical Infrastructure Protection*, chaps. 6-9.

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

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

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

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

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

Congressional Research Service, *Nuclear Power Plants: Vulnerability to Terrorist Attack*, August 8, 2007, <http://www.au.af.mil/au/awc/awcgate/crs/rs21131.pdf>.

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

Federal Emergency Management Agency, *The Voluntary Private Sector Preparedness Program—PS-Prep & Small Business Preparedness*, <http://www.fema.gov/ps-preptm-voluntary-private-sector-preparedness>.

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

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

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

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

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

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

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

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

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

*NIPP Sector Specific Plans*, <http://www.dhs.gov/sector-specific-plans> (assign to different students)

**Lesson 5 topic: Discerning the 21st Century Risk Environment**

**1. Lesson Goal(s)/Objective(s)**:

* Explain how various all-hazards threats may impact critical infrastructure across the critical infrastructure sectors, across all levels of government, and within the private sector.

**2. Discussion Topics**:

* Define “all hazards.”
* How do you define the 21st century threat environment? What is the primary characteristic of this environment? What are the challenges? Where do you get information regarding the current threat environment?
* Why is understanding the threat environment important for critical infrastructure security and resilience?
* Define “target sets” and “asymmetrical warfare.” What part do our critical infrastructure “target sets” play in the concept of “asymmetric warfare?”
* How does the threat impact strategy and planning 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?
* How do international supply chains complicate traditional approaches to risk assessment and management?
* How can tools such as Geographic Information Systems be used to combat threats to critical infrastructure?
* Can we afford the cost of maintaining an all-hazards critical infrastructure preparedness posture?

**3. Required Reading**:

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

Lewis, *Critical Infrastructure Protection in Homeland Security*, chap. 3 and chap. 13, pp. 397-401.

U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, pp. 9-10, 2013, <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.

Congressional Research Service, *International Terrorism and Transnational*

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

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

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

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

Angela Rabasa et. al., “The Lessons of Mumbai,” *RAND Corporation* (2009), <http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP249.pdf>.

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

Xavier Guiho, Patrick Lagadec, and Erwan Lagadec, “Non-Conventional Crises and Critical Infrastructure: Katrina,” *EDF* (2006), [http://www.patricklagadec.net/fr/pdf/EDF-Katrina-Report-31.pdf.](http://www.patricklagadec.net/fr/pdf/EDF-Katrina-Report-31.pdf)

Louise K. Comfort and Thomas W. Haase, “Communication, Coherence, and Collective Action: The Impact of Hurricane Katrina on Communications Infrastructure,” University of Pittsburgh (2006), [http://www.iisis.pitt.edu/publications/Communication\_Coherence\_and\_Collective\_‌Action-Katrina.pdf](http://www.iisis.pitt.edu/publications/Communication_Coherence_and_Collective_%E2%80%8CAction-Katrina.pdf).

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

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

<http://www.fas.org/sgp/crs/misc/RL31873.pdf.>

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

**Lesson 6 Topic: Assessing Critical Infrastructure Risk in an Interdependent World**

**1. Lesson Goal(s)/Objective(s)**:

* Critique the DHS strategic risk assessment process, as well as how other government and private sector critical infrastructure stakeholders view and evaluate risk.
* Examine how risk does or does not drive risk management strategies, plans, and resource investment across government and the private sector.

**2. Discussion Topics**:

* How are the elements of risk 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 security and resilience relate to the concept of risk?
* How does the Federal government assess risk and communicate the results of the risk assessment process to other critical infrastructure stakeholders? Do these other players have a role to play in government risk assessment processes and programs?
* How does risk management relate to strategic decisions, planning, and resource investments in the critical infrastructure security and resilience mission area?
* Is there room for subjectivity in the risk analysis process?
* How does the issue of critical infrastructure dependencies/interdependencies complicate the risk assessment process? How do we measure the dependencies factor? How do we factor interdependencies into the planning process?
* Can we ever get to a totally risk-based critical infrastructure security and resilience construct?
* Should we base the allocation of critical infrastructure -related grant funding on the notion of risk? Is the system working?
* Do the uncertainties surrounding risk quantification hinder our intuitive understanding of risk?

**3. Required Reading**:

Collins and Baggett, *Homeland Security and Critical Infrastructure Protection*, chap. 5.

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

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

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

[http://www.libertysecurity.org/IMG/pdf/CRS\_Report\_-\_‌What\_makes\_an\_Infrastructure\_](http://www.libertysecurity.org/IMG/pdf/CRS_Report_-_%E2%80%8CWhat_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 Program, *Critical Infrastructure Protection: Elements of Risk*, chaps. 2-3, <http://cip.gmu.edu/archive/archive/RiskMonograph_1207_r.pdf>.

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

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

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

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

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

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

**Lesson 7 Topic: Collapse: A Case Study of the 2007 Minneapolis I-35W Bridge Disaster**

Today’s class includes an in-class analysis of the 2007 Minneapolis bridge collapse. Prior to class, please read the case narrative but do not complete the exercises.

**1. Lesson Goal(s)/Objective(s)**:

* Utilize critical infrastructure security and resilience planning and response capabilities to identify and assess threats and vulnerabilities of critical infrastructure located at the nexus of multiple infrastructure modes.

**2. Discussion Topics**:

* See “Key Questions” and “Analytic Value Added” sections in Case Study Narrative.

**3. Required Reading**:

Collapse: A Case Study of the 2007 Minneapolis I-35W Bridge Disaster, http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/Collapse-Learner-Version\_June-2013-Update1.pdf

**Lesson 8 Topic: Recognizing Cyber Threats and SCADA Vulnerabilities**

**\*Special Activity: “Collapse” reflection papers due to Instructor/Professor**

**1. Lesson Goal(s)/Objective(s)**:

* Assess the linkages between cybersecurity and critical infrastructure security and resilience from an operational and security perspective.
* Identify and evaluate the challenges represented by information technology and Supervisory Control and Data Acquisition (SCADA) systems vulnerabilities.
* Analyze how cyber risk is assessed and managed within the various critical infrastructure sectors, as well as how cyber security performance is evaluated.

**2. Discussion Topics**:

* What are the principal threats and challenges of cybersecurity as they pertain to critical infrastructure security and resilience? Is this a “real and present danger?” Why or why not?
* What is SCADA? How do SCADA concerns relate to the critical infrastructure sectors?
* 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 security and resilience-focused strategies and plans?
* How is planning in the cyber domain different from conventional domains?
* What is the correct approach to the integration of physical and cyber assets?

**3. Required Reading**:

Collins and Baggett, *Homeland Security and Critical Infrastructure Protection*, chap. 10.

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

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

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

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

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

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

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

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

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

David Watts, “Security & Vulnerability in Electric Power Systems,” *North American Power Symposium*, 2003, <http://web.ing.puc.cl/~power/paperspdf/WattsSecurity.pdf>.

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

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

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

**Lesson 9 Topic: Building Partnerships and Sharing Information**

**1. Lesson Goal(s)/Objective(s)**:

* Evaluate the methods, processes, and systems that the various critical infrastructure security and resilience partners use to share information with one another, as well as the ongoing challenges and barriers to information sharing and collaboration that exist between all levels of government and the private sector.

**2. Discussion Topics**:

* What are the key elements of the NIPP partnership model? How effective is this model in achieving the necessary level and quality of information sharing required to execute the critical infrastructure security and resilience mission?
* How does one go about the process of building a public-private partnership network or coalition for critical infrastructure security and resilience purposes?
* Does the Critical Infrastructure Partnership Advisory Council (CIPAC) structure facilitate strategy and plan development within the critical infrastructure protection and resilience community?
* What are the Information Sharing and Analysis Centers (ISACs)? How do they interact with government? What role do they play in critical infrastructure security and resilience planning and incident management? Are they effective? In all sectors?
* What are the principal barriers to sharing information proactively and comprehensively between government and industry at all levels of the NIPPpartnership framework?
* What are the principal types and sources of information that support the critical infrastructure security and resilience mission?
* What are the key processes and systems used to share critical infrastructure security and resilience-related data, 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? What areas need 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 the President’s mandate of “no lobbyist” in SCC affect the NIPP partnership?

**3. Required Reading**:

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

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

U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, chap. 4 and app’x 5(a)-(b), 2013, <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.

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

U.S. Department of Homeland Security, *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level*, September 2008, <http://www.dhs.gov/xlibrary/assets/nipp_srtltt_guide.pdf> (see section titled “Critical Infrastructure and Key Resource Protection Capabilities for Fusion Centers”).

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

“The Role of Information Sharing and Analysis Centers (ISACs) in Private/Public Sector Critical Infrastructure Protection,” *ISACCouncil.org*, 2009,

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

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

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

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

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

**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>.

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

**Lesson 10 Topic: Derailed: A Case Study of the 2001 Howard Street Tunnel Fire**

Today’s class includes an in-class analysis of the 2001 Howard Street Tunnel freight train derailment. Prior to class, please read the case narrative and complete Exercise 1.

**1. Lesson Goal(s)/Objective(s)**:

* Identify and assess affected sectors, assets, and stakeholders in the face of a critical infrastructure incident.
* Apply critical infrastructure security and resilience information sharing methods, processes, and systems.

**2. Discussion Topics**:

* See “Key Questions” and “Analytic Value Added” sections in Case Study Narrative.

**3. Required Reading**:

Derailed: A Case Study of the 2001 Howard Street Tunnel Fire, <http://cip.gmu.edu/wp-content/uploads/2013/06/Derailed-Learner-Version.pdf>.

**Lesson 11 Topic: Blackout: A Case Study of the 2003 North American Power Outage**

**\*Special Activity: “Derailed” reflection papers due to Instructor/Professor**

Today’s class includes an in-class analysis of the 2003 northeast blackout. Prior to class, please read the case narrative but do not complete the exercises.

**1. Lesson Goal(s)/Objective(s)**:

* Identify and evaluate the effects of cascading failures and interdependencies resulting from a critical infrastructure incident.
* Generate various futures scenarios and assess their implications for critical infrastructure security and resilience.

**2. Discussion Topics**:

* See “Key Questions” and “Analytic Value Added” sections in Case Study Narrative.

**3. Required Reading**:

Blackout: A Case Study of the 2003 North American Power Outage, http://cip.gmu.edu/wp-content/uploads/2013/10/blackout-learner-version.pdf

**Lesson 12 topic: Incident Management Exercise**

**\*Special Activity: “Blackout” reflection papers due to Instructor/Professor**

**\*\*Special Activity: Incident Management Point Paper due to Instructor/Professor**

Today’s class involves a 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 FSLTT 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 security and resilience-related communication and information sharing, coordination, integration of capabilities, and problem identification and resolution. A complete outline of the exercise is located at **Attachment 1**.

**1. Lesson Goals/Objectives**:

* Analyze the respective responsibilities and evaluate the implications for critical infrastructure security and resilience of varying courses of action that may be followed by government, the private sector, and the general public.
* Assess the functionality and contributions of the critical infrastructure incident management nodes, coordinating structures, and the processes through which they interact.
* Assess the security, economic, and social implications that may arise from changes in the national threat level through the National Terrorism Advisory System (NTAS).

**2. Discussion Topics**:

* What doctrine or principles govern or guide critical infrastructure owners and operators and government both for steady-state security and resilience and response to natural disasters, manmade hazards, or terrorist threats?
* How are the concepts of prevention, protection, mitigation, response, and recovery relating to critical infrastructure addressed at various levels of government? How are these concepts reflected in business practices by critical infrastructure owners and operators?
* What are the roles and responsibilities of the various public and private partners vis-à-vis national incident management?
* Define the concept of “whole of community” or “all or nation” and explain the relevance or significance for critical infrastructure.
* What are the elements of National policy or doctrine that apply in these situations?
* In the context of National Preparedness, what core capabilities are required to ensure critical infrastructure preparedness? How are these addressed in the National Preparedness goal and National Frameworks? How do these relate to the NIPP?
* How are information and intelligence shared between the various public and private sector nodes in an emergent threat scenario? Does the process work?
* How does the 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?

**3. Required Reading**:

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

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

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

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

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

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

1. **Additional Recommended Reading**

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

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

**Lesson 13 topic: Collaborative Planning Project Presentations**

**1. Lesson Goals/Objectives**:

* Provide the highlights and foster classroom discussion of the critical infrastructure security and resilience strategy, plan, or program developed by the Planning Team(s).

**2. Discussion Topics**:

* Planning Team presentations

**3. Required Reading**:

* As required for project development and presentation

**Lesson 14 topic: Collaborative Planning Presentations**

**1. Lesson Goals/Objectives**:

* Provide the highlights and foster classroom discussion of the critical infrastructure security and resilience strategy, plan, or program developed by the Planning Team(s).

**2. Discussion Topics**:

* Planning Team presentations

**3. Required Reading**:

* As required for research paper and presentation

**Lesson 15 Topic: Evaluating the Future of Critical Infrastructure Security and Resilience**

**1. Lesson Goal(s)/Objective(s)**:

* Identify and assess evolving and future threats to critical infrastructure.
* Analyze the strategic choices that may impact our approach to critical infrastructure security and resilience planning in the medium-long term future.
* Evaluate the requirements for critical infrastructure security and resilience awareness, education, and training programs today and in the future.

**2. Discussion Topics**:

* What insights do we have on the nature of future critical infrastructure dependencies and interdependencies?
* Can the future world of critical infrastructure security and resilience be simulated and “war-gamed” today?
* What actions should we be taking now to buy down future risk and position the next generation for success in this issue area? Will today’s priority focus areas set us up for success? Are we focused on the right things moving forward?
* What are the metrics that will guide relevant critical infrastructure security and resilience feedback processes in the future?
* How are critical infrastructure security and resilience-related requirements determined and resourced within government? Industry? Across sectors? Are these processes sufficient to get us ready for the future?
* How do we begin to address planning concerns that transcend the next budget cycle?
* How can we achieve truly integrated critical infrastructure security and resilience planning in the future? How can critical infrastructure security and resilience goals and objectives be harmonized within and across sectors, jurisdictions, and geographic regions?
* What are the core elements of an effective critical infrastructure security and resilience awareness, education, and training program?
* What are the keys to effective critical infrastructure security and resilience program management today and in the future?

**3. Required Reading**:

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

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

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

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

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

**ATTACHMENT 1**

**CRITICAL INFRASTRUCURE SECURITY AND RESILIENCE INCIDENT MANAGEMENT EXERCISE**

**TERRORISM SCENARIO**

**Module 1: Pre-Incident**

1. **Scenario Build**
* A new video is released by a well-known terrorist organization on several internet sites. The video describes “striking the infidels where they are most vulnerable,” using advanced weapons and tactics. The spokesperson references the possibility of attacks targeting European and American interests worldwide, with particular emphasis on transportation, commercial facilities and sports venues, religious worship sites, iconic symbols, financial centers, and government buildings.
* Daily news reports include brief mention of the video. 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.
* Violent extremist group Internet “chatter” and known-terrorist-organization’s website activities 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.
1. **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 terrorist organization. He states that his planned attack was to serve as a warning to all countries with “Criminals assaulting his god.” He is quoted as saying “When the criminal governments fall, we 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.
1. **Discussion Questions**
* 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, mass transit, 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 television by an affiliate with known terrorist 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, as well as for the geographical areas of the National Capital Region and New York State Region.
1. **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. Two 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 a terrorist 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?