**Course Number: XXXX**

**Course: Introduction to Critical Infrastructure Security 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 21st 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 security and resilience from an all-hazards perspective. It describes the strategic context presented by the 21st 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 security and resilience, applicable to the different 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. Explain the evolution of critical infrastructure security and resilience as a core homeland security policy area**:

* The history of critical infrastructure security and resilience as a policy focus area, overarching policy approaches, and implications for policy making today
* Executive, congressional, and judicial engagement in the critical infrastructure security and resilience mission space
* Real-world incidents as focusing events

**2. Assess the 21st century risk environment and its application to the critical infrastructure security 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. Identify and evaluate the roles and responsibilities of key critical infrastructure security and resilience public and private sector stakeholders:**

* Federal, State, local, tribal, territorial, regional, and private sector stakeholders
* International stakeholders
* Influence of regulations and formal and informal incentives
* Sensitivity to different perspectives and taxonomies

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

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

**5. Compare different strategic approaches to and issues regarding critical infrastructure risk management, including: risk analysis, cost-benefit analysis, risk mitigation, and performance measurement (regulatory and non-regulatory):**

* Physical and cyber assets
* Cybersecurity
* Insider threats (including personnel security)
* Systems dependencies/interdependencies
* Jurisdictional considerations
* Sector approaches

**6. Recognize the complexities associated with effective and efficient critical infrastructure security and resilience program management in a dynamic risk and future operating environment:**

* Developing sector-specific, jurisdictionally-based, or regionally-focused critical infrastructure security and resilience goals, objectives, risk mitigation approaches, and plans
* Designing and applying continuous feedback mechanisms to measure critical infrastructure security and resilience program performance
* Designing and implementing critical infrastructure security and resilience awareness, education, and training plans and programs
* Doing more with less: critical infrastructure security 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 15%

(Player Roles and Responsibilities Paper)

**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 security 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 security 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 security and resilience sector or sub-sector level plan; critical infrastructure security and resilience regional, State or municipal-level critical infrastructure security and resilience plan; or Federal-level critical infrastructure security and resilience plan or policy. Learner critiques should include alternative visions/strategies for successful critical infrastructure security 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 security 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 students 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. (ed.), *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 Security and Resilience**

**1. Lesson Goals/Objectives:**

* Review the scope of the course, administrative requirements, instructional methodology, evaluation criteria, feedback processes, and learners’ field of study.
* Define and identify critical infrastructure.
* Recognize critical infrastructure security and resilience as a multidisciplinary field and the advantages/disadvantages this creates.
* Explain how critical infrastructure security and resilience policy and structural organization have changed as a function of the all-hazards risk environment over time, including specific threats and hazards.

**2. Discussion Topics:**

* What are critical infrastructures and why are they important to us?
* Why does critical infrastructure security and resilience represent such a challenge?
* How has the critical infrastructure security and resilience mission changed over time from a historical perspective?
* What are the general principles we typically associate with critical infrastructure security and resilience in the U.S. context?
* How has the Nation’s approach to critical infrastructure security and resilience changed over time with regard to certain threats/hazards?
* How would you characterize critical infrastructure security 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 security and resilience over the years?
* How does the U.S. Congress view the critical infrastructure security and resilience mission area? Does legislation clarify or complicate the critical infrastructure security and resilience mission space?
* Where should the next Administration/Congress take the critical infrastructure security and resilience mission area?

**3. 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*, 2014, <http://www.fas.org/sgp/crs/homesec/RL30153.pdf>.

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

The White House, *National Security Strategy*, May 2010, <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.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.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, pp. 1-10, 13-14, <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>.

U.S. Department of Homeland Security, *Quadrennial Homeland Security Review, 2014*, <http://www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.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>.

*National Strategy for Homeland Security*. 2007. <http://www.hsdl.org/?view&did=479633>

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: Achieving Critical Infrastructure Resilience**

**1. Lesson Goals/Objectives:**

* Explain the concept of resilience and its application to the critical infrastructure arena.
* Identify and evaluate strategies and initiatives currently underway to enhance critical infrastructure resilience across all government levels, as well as the private sector.

**2. Discussion Topics:**

* What is the concept of “resilience” as it applies to critical infrastructure security and resilience?
* Are “security” and “resilience” mutually exclusive concepts?
* What are the general principles associated with resilience as currently applied within government and industry?
* Discuss the similarities and differences between operational resilience, community resilience, organizational resilience, and personal resilience. How are they related?
* 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?
* How does NIPP 2013 define resilience for critical infrastructure?
* How is resilience measured? How should it be?

**3. Required Reading:**

Brandon J. Hardenbrook, *The Need for a Policy Framework to Develop Disaster Resilient Regions,* 2005, <http://www.degruyter.com/view/j/jhsem.2005.2.3/jhsem.2005.2.3.1133/jhsem.2005.2.3.1133.xml>.

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

T.D. O’Rourke, *Critical Infrastructure, Interdependencies and Resilience,* Spring 2007,

<http://www.nae.edu/File.aspx?id=7405>.

Brian Jackson, *Marrying Prevention and Resiliency*, 2008, <http://www.rand.org/pubs/occasional_papers/2008/RAND_OP236.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>.

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>.

National Infrastructure Advisory Council, *Optimization of Resources for Mitigation of Infrastructure Disruption Study Final Report and Recommendations,* October 19, 2010, <http://www.dhs.gov/xlibrary/assets/niac/niac-optimization-resources-final-report-10192010.pdf>.

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

The Infrastructure Security Partnership, *Understanding Resilience: Disaster Resilience Begins with You*, July 30, 2013, <http://www.tisp.org/index.cfm?cdid=13180&pid=10261>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 12(6), December 2013, <http://cip.gmu.edu/wp-content/uploads/2014/01/December-2013_Resilience.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 12(7), January 2014, <http://cip.gmu.edu/wp-content/uploads/2013/06/January-2014_Resilience.pdf>.

**Lesson 3 topic: Examining Critical Infrastructure Security and Resilience in the Context of the 21st Century Risk Environment**

**1. Lesson Goals/Objectives:**

* Identify and evaluate the various threats and hazards that may impact critical infrastructure within and across the different sectors, and how they can be viewed in an all-hazards risk management approach.
* Assess the challenges associated with critical infrastructure security 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?
* 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 security and resilience?

**3. Required Reading:**

Brown, Chapter 5.

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

Collins and Baggett, Chapters 13-15.

Strategic National Risk Assessment Executive Summary, 2012, <http://www.fema.gov/media-library/assets/documents/29223>.

Post-Katrina Emergency Management Reform Act of 2006, <http://www.govtrack.us/congress/bills/109/s3721>.

Xavier Guiho, Patrick Lagadec and Erwan Lagadec,

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

Louise K. Comfort and Thomas W. 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>.

Robert A. Miller and Irving Lachow, 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>.

Brian Jackson and David Frelinger, *Emerging Threats and Security Planning*,2009, <http://www.rand.org/pubs/occasional_papers/2009/RAND_OP256.pdf>.

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

Congressional Research Service Report, *International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress*, 2010,

<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*,2010,

<http://www.fas.org/sgp/crs/terror/R41070.pdf>.

The 9/11 Commission Report, *Final Report of the National Commission on Terrorist Attacks Upon the United States*, Chapters 2, 3, 6 and 7, 2004

<http://www.9-11commission.gov/>.

Atomic Energy Society of Japan, “*Lessons Learned from the Accident at the Fukushima Daiichi Nuclear Power Plant*,” 2011, <http://www.aesj.or.jp/en/release/gbcom_kyokun_EN_20110530.pdf>.

Jack Spencer, “*U.S. Nuclear Policy after Fukushima: Trust but Modify*,” Backgrounder No. 2557, The Heritage Foundation, 2011, <http://thf_media.s3.amazonaws.com/2011/pdf/bg2557.pdf>.

The 2012 Critical Infrastructure Symposium: *Lessons Learned from Past Attacks on America’s Infrastructure*,Raymond H. Bennett, Ph.D., P.E., Baker Engineering and Risk Consultants Inc., 2011

<http://tisp.org/index.cfm?pid=12831>.

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>.

**Lesson 4 topic: Examining Critical Infrastructure Security 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:**

* Identify key stakeholders within the critical infrastructure security and resilience mission space and discuss the roles and responsibilities of each.
* Examine the differences between regulated and voluntary regimes across the critical infrastructure sectors.
* Evaluate the principal political, organizational, legal, and resource challenges that those responsible for critical infrastructure security and resilience face in executing those responsibilities.

**2. Discussion Topics:**

* Who is “in charge” of critical infrastructure security and resilience nationally, regionally, locally, and across the critical sectors?
* What are the key roles and responsibilities of the following with respect to critical infrastructure security 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 security and resilience 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 critical infrastructure sectors organized to accomplish the critical infrastructure security and resilience mission at the sector and sub-sector levels? What is their “motivation” regarding their role in executing the critical infrastructure security and resilience mission?
* How does the distributed structure of critical infrastructure security and resilience responsibility and accountability play out against the principal threats we face in this mission area?

**3. Required Reading:**

Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, February 12, 2013,

<http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, pp. 10-12, Appendix B, 2013, <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.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>.

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

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

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

**Lesson 5 topic: Organizing and Partnering for Critical Infrastructure Security and Resilience and networking to Share Information**

**1. Lesson Goals/Objectives:**

* Identify and assess the different methods, processes, and systems that the various critical infrastructure security and resilience partners use to share information with one another.
* Evaluate the ongoing challenges and barriers to information sharing and collaboration that exist among the various levels of government, as well as between government and the private sector.
* Discuss how critical infrastructure security 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 security 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 security and resilience mission?
* What are the key processes and systems used to share critical infrastructure security and resilience -related data, to include intelligence-related information, among the various stakeholders nationally, regionally, and locally?
* How is classified national security information shared between government and industry? How and from whom does industry receive terrorism-related information?
* How do government and industry work together to protect sensitive information? Are there areas for improvement?
* What are the roles and responsibilities of 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 security and resilience information sharing and analysis?
* How are critical infrastructure security and resilience information and intelligence that originate from multiple distributed sources compiled and deconflicted? Are we successfully “connecting the dots” today?
* How have real-world successes/failures led to improvements in information sharing among government and industry partners?

**3. Required Reading:**

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, Appendix A, <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>.

*A Policy Framework for the ISAC Community*,2004,

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

*National Strategy for Information Sharing*, 2007,

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

National Infrastructure Advisory Council, *Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations*, 2008, <http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf>.

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>.

Robert Riegle, Testimony, *The Future of Fusion Centers: Potential Promise and Dangers*, 2009, <http://www.dhs.gov/ynews/testimony/testimony_1238597287040.shtm>.

*The Role of ISACs in Private/Public Sector CIP*, 2009,

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

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 8(11), 2010, <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_May2010_InformationSharing.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 2013, 11(10), pp. 1-8, 16-21, 2013, <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/April2013_PartershipsInformationSharing.pdf>.

*Information Sharing and the Private Sector,* <http://www.ise.gov/sharing-private-sector>.

*Information Sharing Environment*,<http://itlaw.wikia.com/wiki/Information_Sharing_Environment>.

National Strategy for Information Sharing and Safeguarding, 2012, <http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf>.

**4. Recommend Additional Reading:**

CIKR Resource Center, *CIKR Partnerships*.

<http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/CIKRpartnerships.htm>.

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

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

**1. Lesson Goals/Objectives:**

* Define the major elements of risk in the context of critical infrastructure security and resilience: threats, vulnerabilities, and consequences
* Critique the NIPP strategic risk management process, as well as how other government and private sector critical infrastructure stakeholders view and evaluate risk
* Explain how risk drives risk management strategies, plans, and resource investment across government and the private sector
* Explain how critical infrastructure security and resilience-focused risk differs from that applied in the context of other disciplines (security, engineering, finance, and business)
* Compare and contrast terrorism risk and the risk represented by natural disasters and other manmade hazards
* Evaluate the complexities regarding critical infrastructure dependencies and interdependencies as they relate to risk and its components

**2. Discussion Topics:**

* What are the major elements of risk as they pertain to the critical infrastructure security 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 security 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 security 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 security and resilience mission area?
* How do we calculate risk across threat/hazard types? Across jurisdictions? Across sectors?
* Is there room for subjectivity in the risk analysis process?
* How does the issue of critical infrastructure dependencies/interdependencies complicate the risk assessment process? How do we measure these dependencies and interdependencies?
* Can we ever get to a completely 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?

**3. Required Reading:**

Collins and Baggett, Chapter 5.

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

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, pp. 15-20,

<http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>

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

Y.Y. Haimes, “Infrastructure Interdependencies and Homeland Security,” *ASCE Journal of Infrastructure Systems*, 11(2), 2005, 65-66.

<http://www.wou.edu/~koboldm/RCTP/RCTP%20Resource%20Handbook/Haimes_infrastructure_interdependencies_and_homeland_securit.pdf>.

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

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

George Mason University, The Center for Infrastructure Protection and Homeland Security, *Critical Infrastructure Protection: Elements of Risk*,Various articles, 2007,

<http://cip.gmu.edu/wp-content/uploads/2014/03/ElementsofRiskMonograph.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>.

DHS, “Risk Lexicon,” <http://www.fema.gov/pdf/government/grant/2011/fy11_hsgp_lexicon.pdf>.

U.S. Government Accountability Office, *Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities*,2011,<http://www.gao.gov/new.items/d11537r.pdf>.

George Mason University, Center for Infrastructure Protection and Homeland Security (CIP/HS), *The CIP Report*, 10(2), 2011,

<http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_August2011_Interdependencies.pdf>.

Michel Van Eeten, Albert Nieuwenhuijs, Eric Luiijf, Marieke Klaver, and Edite Cruz, “The State and the Threat of Cascading Failure across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports,” *Public Administration*, 89(2), 2011, 381–400,

<http://onlinelibrary.wiley.com/doi/10.1111/j.1467-9299.2011.01926.x/abstract>.

**Lesson 7 topic: Enabling Security, 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 nipp sector-specific plans (ssps). individual ssp reading assignments will be made by the instructor at the end of the previous lesson,** <http://www.dhs.gov/critical-infrastructure-sectors>.

**1. Lesson Goals/Objectives:**

* Explain the strengths and weaknesses of the voluntary approach to critical infrastructure security and resilience.
* Evaluate how risks are assessed and managed and how performance is measured in those sectors in which security is not regulated by a government entity.
* Identify and discuss the various resources made available by the Federal government to other levels of government and the private sector to foster critical infrastructure security 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 security 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 security 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.

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

Daniel Prieto, *Mass Transit after the London Bombings*, 2005, <http://belfercenter.ksg.harvard.edu/publication/3275/mass_transit_security_after_the_london_bombings.html?breadcrumb=%2Fexperts%2F812%2Fdaniel_b_prieto>.

Bill Johnstone, *New Strategies to Protect America: Terrorism and Mass Transit after London and Madrid*, 2007,

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

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

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

**4. Additional Readings** (See above for special instructions):

*NIPP Sector Specific Plans* (Communications, Defense Industrial Base, Energy, Financial Services, Food and Agriculture, Information Technology, Transportation Systems, and Water and Wastewater Systems) located at <http://www.dhs.gov/critical-infrastructure-sectors>

**Lesson 8 topic: Enabling Protection, Managing Risk, and Measuring Performance: The Regulatory Approach**

**1. Lesson Goals/Objectives:**

* Explain the strengths and weaknesses of the regulatory approach to critical infrastructure security and resilience.
* Evaluate how risks are assessed and managed and how performance is measured in those sectors in which security, emergency preparedness, and emergency response are regulated by a government entity.
* Identify and discuss the differences in the approaches used in the regulated sectors: chemical/hazardous materials, freight rail, aviation, ports, commercial and nuclear facilities, electricity, and financial services.

**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 security 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.

Public Law 107-295, *Maritime Transportation Security Act of 2002*,

http://www.gpo.gov/fdsys/pkg/PLAW-107publ295/content-detail.html.

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

Mark Holt and Anthony 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/homesec/RL33347.pdf>.

*Security Spotlight*, 2008, <http://www.nrc.gov/security.html>.

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>.

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>.

George Mason University, The Center for Infrastructure Protection and Homeland Security (CIP/HS), *The CIP Report*, 10(3), September 2011,

<http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_September2011_9_11_10thAnniversary.pdf>.

**Lesson 9 topic: Cybersecurity and** Supervisory Control and Data Acquisition **(SCADA) Vulnerabilities: Identifying and Managing “Nanosecond” Risk and Performance**

**1. Lesson Goals/Objectives:**

* Examine the linkages between cybersecurity and critical infrastructure security and resilience from an operational and security perspective.
* Identify and evaluate the challenges presented by information technology and SCADA systems vulnerabilities.
* Explain how cyber risk is assessed and managed within the various critical infrastructure sectors, as well as how cybersecurity risk mitigation 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?
* How has the White House addressed the cyber problem? Has its approach been effective? 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.

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

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

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

Jason Stamp, Phil Campbell, Jennifer DePoy, John Dillinger, and William Young, *Sustainable Security for Infrastructure SCADA*,2003, <http://energy.sandia.gov/wp/wp-content/gallery/uploads/SustainableSecurity.pdf>.

David Watts, *Security and Vulnerability in Electric Power Systems*, 2003,

http://web.ing.puc.cl/~power/paperspdf/WattsSecurity.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>*.*

Peter Allor, *Understanding and Defending Against Foreign Cyber Threats*, (2007),

<http://www.homelandsecurity.org/journal/Default.aspx?oid=165&ocat=1>.

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>.

Mariana Hentea, *Improving Security for SCADA Control Systems*, 2008,

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

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>.

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>.

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

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 9(7), January 2011, <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_January2011__Cybersecurity.pdf>.

United Kingdom Cyber Security Strategy, <http://www.carlisle.army.mil/dime/documents/UK%20Cyber%20Security%20Strategy.pdf>.

MELANI, “Reporting and Analysis Centre for Information Assurance,” <http://www.melani.admin.ch/index.html?lang=en>.

United Nations General Assembly, *International Code of Conduct for Information Security*, <http://www.rusemb.org.uk/policycontact/49>.

**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%282007%29.pdf).

**Lesson 10 topic: The International Dimension of Critical Infrastructure Security and Resilience**

**1. Lesson Goals/Objectives:**

* Identify and discuss the international dimensions of critical infrastructure security and resilience.
* Summarize alternative approaches to critical infrastructure security and resilience in use internationally, including voluntary and regulatory models.
* Identify and examine various structures and forums that are used to promote international critical infrastructure security and resilience cooperation and collaboration.

**2. Discussion Topics:**

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

**3. Required Reading:**

Arjen Boin, Mark Rhinard, and Magnus Ekengren,

*Institutionalizing Homeland Security Cooperation in Europe*,2007,

<http://citation.allacademic.com/meta/p_mla_apa_research_citation/2/1/0/1/5/pages210155/p210155-1.php>

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

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

Infrastructure Canada*,*

*Literature Review of Methodology to Evaluate the State of Infrastructure*, August 2007,

<http://books1.scholarsportal.info/viewdoc.html?id=25360>

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>.

International CIIP Handbook (2008-2009), <https://www.hsdl.org/hslog/?q=node/4413>.

European Commission, *Protecting Europe from Large-scale Cyber attacks and Disruptions: Enhancing Preparedness, Security and Resiliency*, 2009,

<http://europa.eu/legislation_summaries/information_society/internet/si0010_en.htm>

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

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

Public Safety Canada, *National Strategy for Critical Infrastructure and Action Plan for Critical Infrastructure*, 2010,

<http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-eng.pdf>.

U.S. Department of Homeland Security and Public Safety Canada, *Canada-United States Action Plan for Critical Infrastructure*, 2010,

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

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

George Mason University, The Center for Infrastructure Protection and Homeland Security (CIP/HS), *The CIP Report*, 9(12), June 2011,

<http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_June2011_InternationalCIP.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security (CIP/HS), *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>.

National Strategy for Global Supply Chain Security, January 2012,

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

”Trusted Information Sharing Network,” <http://www.tisn.gov.au/Pages/default.aspx>

“Center for the Protection of National Infrastructure,” <http://www.cpni.gov.uk/>.

“Infrastructure Canada,” [www.infrastructure.gc.ca](http://www.infrastructure.gc.ca)..

**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 the 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 security 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:**

* Evaluate the processes and mechanisms used to build situational awareness and facilitate government-private critical infrastructure-related prevention, protection, mitigation, response, and recovery activities.
* Identify critical infrastructure security laws, policies, and programs with application to the management of emergent threats and 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:**

Review the NIPP 2013 Partnership and Risk Management Framework, <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>.

Department of Homeland Security, “National Terrorism Advisory System,” <http://www.dhs.gov/files/programs/ntas.shtm>.

U.S. Department of Homeland Security, *Overview of the National Planning Frameworks*, (May 2013). <http://www.fema.gov/media-library-data/20130726-1914-25045-2057/final_overview_of_national_planning_frameworks_20130501.pdf>.

U.S. Department of Homeland Security, *National Response Framework*, 2013,

<http://www.fema.gov/media-library/assets/documents/32230?id=7371http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf>.

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>.

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

**4. Additional Recommended Reading:**

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

**Lesson 12 topic: Critical Infrastructure Security 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>.

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>.

**Lesson 13 topic: Student Presentations (Student Activity)**

**1. Lesson Goals/Objectives:**

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

**2. Discussion Topics:**

* Student presentations

**3. Required Reading:**

* As required for research paper and student presentation

**Lesson 14 topic: Student Presentations (Student Activity)**

**1. Lesson Goals/Objectives:**

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

**2. Discussion Topics:**

* Student presentations

**3. Required Reading:**

* As required for research paper and student presentation.

**Lesson 15 topic: Managing an effective Critical Infrastructure Security 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:**

* 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.
* Discuss the requirements for critical infrastructure protection and resilience awareness, education, and training programs today and in the future.

**2. Discussion Topics:**

* What will the critical infrastructure security and resilience operational environment look like 10-20 years from now?
* What will be the principal threats and challenges to critical infrastructure security 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 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 area? Will today’s priorities set us up for success?
* 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 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:**

Rand Corporation, *Cyber-terrorism: The Threat of the Future?* Rand Corporation Summary Report, 2003, <http://www.rand.org/pubs/reprints/RP1051.html>.

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>.

Bob Prieto, *Infrastructure Resiliency: Do We Have the Focus Right?* November 16, 2009,

<http://www.tisp.org/index.cfm?cdid=11838&pid=10261>.

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

Brian Vastag, “As the Sun Awakens, the Power Grid Stands Vulnerable,”

*Washington Post*, June 20, 2011, <http://www.washingtonpost.com/national/science/as-the-sun-awakens-the-power-grid-stands-vulnerable/2011/06/09/AGwc8DdH_story.html?hpid=z2>.

International Atomic Energy Agency, *Report of Japanese Government to IAEA Ministerial Conference on Nuclear Safety-Accident at TEPCO’d Fukushima Nuclear Power Stations*,June 7, 2011, <http://www.iaea.org/newscenter/focus/fukushima/japan-report/>.

U.S. Department of Homeland Security, *Department of Homeland Security Budget*, <http://www.dhs.gov/xabout/budget/dhs-budget.shtm>.

The White House,

*Budget of the United States Government, Fiscal Year 2013: Homeland Security*, <http://www.whitehouse.gov/sites/default/files/omb/budget/fy2013/assets/homeland.pdf>.

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

**ATTACHMENT 1**

**CRITICAL INFRASTRUCURE PROTECTION 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 National Prevention, Protection, and Response Frameworks be doing at this time?

**Module 2: Warning**

1. **Scenario Build**
* During the week after the terrorist attack on the mass transit system in Berlin, the FBI and DHS have received increased reporting of planning for possible near term attacks on commercial facilities, government facilities, national monuments, financial centers, and the transportation sector (highways, rail, 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. issues an Elevated alert under NTAS (or issues a Joint Intelligence Bulletin) 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**
* An imminent alert is issued under NTAS for airports, tunnels and bridges, mass transit, commercial facilities, government facilities and national monuments and icons. All other sectors are under an NTAS elevated alert .
* **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 revising the NTAS alert with guidance 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 cancelling the NTAS alert.
* 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 NTAS alerts 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?