

Course Number: XXXXXX

Course: Critical Infrastructure Protection Methods, Policies, and Strategies

University of XXXXXX

Fall/Spring Semester 20XX

NAME OF SCHOOL:

DEPARTMENT:

PROGRAM:

PROFESSOR:

Telephone Number:

Office Location:

Office Hours:

Email:

Website:

COURSE DESCRIPTION/OVERVIEW:

This course facilitates student-centered learning, integrates critical decision-making, and uses historical event case studies to reinforce national security and homeland security policies governing the protection, identification, and resilience of the Nation's critical infrastructure¹ from an all-hazards context with emphasis on the prevention, mitigation, and response to adversary attack scenarios against single or multiple critical infrastructure sectors.

CREDITS CONFERRED: 3

PREREQUISITE: Introduction to Critical Infrastructure Protection and Resilience

In addition to successfully completing Introduction to Critical Infrastructure Protection and Resilience, each learner is expected to perform graduate-level work, understand basic management principles, and be able to apply appropriate knowledge and techniques to real-world situations. Learners should have the ability to conduct research, compile a list of appropriate sources, analyze the data, and draw conclusions based on that research.

¹ Critical infrastructure is defined as systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any federal, state, regional, territorial, or local jurisdiction (2009 NIPP p. 109).

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

Learner Outcomes: This course is designed to enable learners to:

1. Identify key national security policy shifts and the competition between security, freedom, and privacy since 9/11 that has impacted the definition of critical infrastructure.
2. Examine the roles and responsibilities of the U.S. National Security and Homeland Security Councils in the development, implementation, and management of national strategies for homeland defense and security.
3. Identify the roles and responsibilities of government, private sector, and non-government organizations (NGO) to protect critical infrastructure systems.
4. Analyze key elements needed in an effective physical and cybersecurity protection system and the integration of science and technology to counter and mitigate asymmetric and advanced persistent threats.
5. Understand the need for a dynamic methodology in the prevention, mitigation, and response to an all-hazards approach and continuity of government.

Learning Objectives: This course is designed to prepare learners to:

1. Discuss the rationale for establishing the Department of Homeland Security (DHS), identifying critical infrastructure systems, and publishing Homeland Security Presidential Directives (HSPD).
2. Analyze the national security strategy released by the White House in May 2010 that lays out a strategic approach to secure the Nation against 21st century threats.
3. Develop a working knowledge through the use of case studies of what constitutes critical infrastructure and resilience in preventing, mitigating, and responding to malevolent acts and natural disasters.
4. Defend the need for clear and unambiguous concepts when defining risk terms and risk methodologies for protecting critical infrastructure and the resilience of these assets.
5. Construct critical infrastructure all-hazards and attack scenarios based on postulated threats and historical examples to identify effective countermeasures.
6. Assess the resilience of a given critical infrastructure sector(s), network, or function.
7. Discuss the impact of three supply chain issues on any two sectors of the critical infrastructure during a major incident.

DELIVERY METHOD:

This course features seminar-style discussions — stimulated by lectures and case studies focused on course goals — and learning objectives, both supplemented by current international and national critical infrastructure and resilience all-hazards and security issues selected from the news media and the DHS Blog (<http://blog.dhs.gov>). Learners will have the opportunity to lead class discussions and to make presentations to enhance the learning process.

The assigned course reading include a variety of resources, such as authoritative readings (legislation, executive orders, policies, plans and strategies), implementation readings (government products that are responsive or attempt to fulfill the requirements of authoritative documents), and external reviews (U.S. Government Accountability Office, Congressional Research Service, etc.). Learners are expected to familiarize themselves with the assigned topic and readings before class and should be prepared to discuss and debate them critically as well as analyze them for biases and multiple perspectives.

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. Because the 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. Follow university policy regarding use of beepers and cell phones while class is in session.

GRADING/COURSE REQUIREMENTS:

The three basic requirements for the course are worth a total of 100 points:

1. **Participation:** This will be based on class attendance, completion of assignments, active participation in case studies, and informed contribution to class discussions.
2. **Group Case Studies:** Historical events using a case study methodology will facilitate real-world examples of key teaching points with an emphasis on critical infrastructure lessons learned. Case study format is located at the end of this syllabus.

3. Write a Term Paper: Completion of a 15-20 page term paper.

Class Participation	20%
Group Case Study	20%
Presentations	20%
Term Paper	40%

ACTIVITIES, EXERCISE, AND RESEARCH PROJECTS:

1. Prepare attack and all-hazards scenarios targeting critical infrastructure systems to identify adversary attack scenarios, all-hazards risks, and evaluate countermeasures and resilience.
2. Present group case studies based on a contemporary historical event identifying critical infrastructure issues. Case study topics are identified in the table, *Topics and Case Studies*, page 7.
3. Write term paper on a critical infrastructure protection and resilience topic approved by the instructor and present to the class. Term papers and presentations are scheduled for the last two classes.

INCORPORATION OF FEEDBACK:

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

COURSE READINGS:

The following textbooks are identified as primary textbooks reading 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.

COURSE TEXTBOOKS:

Mary Lynn Garcia. *The Design and Evaluation of Physical Protection Systems*. (2nd edition, 2010).

ARTICLES AND REPORTS:

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, Authorized Edition, Chapter 2, 3, 6 and 7.

<http://www.gpoaccess.gov/911/>.

National Security Strategy, May 2010,

<http://www.whitehouse.gov/> [Search: Issues>Homeland Security].

National Infrastructure Protection Plan: Partnering to enhance protection and resiliency, 2009,

http://www.dhs.gov/files/programs/editorial_0827.shtm.

The National Strategy to Secure Cyberspace, July 2009,

http://www.dhs.gov/files/publications/editorial_0329.shtm.

Critical Infrastructure Sectors,

http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

WEB SITES:

Homeland Security Critical Infrastructure,

<http://www.dhs.gov/files/programs/critical.shtm>.

DHS Risk Lexicon 2010 Edition,

http://www.dhs.gov/files/publications/gc_1232717001850.shtm.

Homeland Security Presidential Directives,

http://www.dhs.gov/xabout/laws/editorial_0607.shtm.

One Team, One Mission, Securing Our Homeland, U.S. Department of Homeland Security Strategic Plan Fiscal Years 2008–2013,

http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf.

The National CI/KR Protection Annual Report, <http://www.dhs.gov/xabout/strategicplan/>
[Additional link within document].

George Mason University Center for Infrastructure Protection and Homeland Security,

<http://cip.gmu.edu/>.

International Issues for CIKR Protection,

http://www.dhs.gov/xlibrary/assets/nipp_international.pdf.

The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets, http://www.dhs.gov/files/publications/publication_0017.shtm.

Homeland Security Presidential Directive 7— Critical Infrastructure Identification, Prioritization, and Protection,
http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1.

U.S. Fire Academy FEMA, Critical Infrastructure Protection,
<http://www.usfa.dhs.gov/fireservice/subjects/emr-isac/index.shtm>.

National Infrastructure Protection: Sector Protection Model,
http://www.dhs.gov/xlibrary/assets/NIPP_InfoSharing.pdf.

Critical Infrastructure and Key Resources Sector Partnership Ethics Guidelines,
<http://podcast.tisp.org/index.cfm?cdid=11046&pid=10261>.

The Monthly Critical Infrastructure Protection Reports (CIP), <http://cip.gmu.edu/>.

Department of Homeland Security's Science and Technology Directorate — Tech Solutions Program, http://www.dhs.gov/xfrstresp/training/gc_1174057429200.shtm.

REFERENCE TEXTBOOKS:

Security Risk Assessment and Management: A Professional Practical Guide for Protecting Buildings and Infrastructure, John Wiley and Son, 2007.

Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, The National Academies Press, Washington, D.C., 2002,
http://books.nap.edu/catalog.php?record_id=10415.

Barabási Albert-László, *Linked: How Everything Is Connected to Everything Else and What It Means*, A Plume Book, (Paperback), 2003.

Joshua Cooper Ramo, *The Age of the Unthinkable: Why the New World Disorder Constantly Surprises Us And What We Can Do About It*, Little, Brown and Company – 2010.

GRADING SCALE (SCHOOL POLICY DEPENDENT):

COURSE TOPICS:

Lesson	Topic and Case Studies*
Lesson 1	Overview National Security and Homeland Security Framework
Lesson 2	Critical Infrastructure Protection and Resilience
Lesson 3	Critical Infrastructure Protection and Resilience: Sector-Specific Plans
Lesson 4	Natural Disasters, Threats, Attack Scenarios, and Countermeasure <i>Case Study</i> <i>Hurricane Katrina, 2005-Challenges: Infrastructure and Assessments</i>
Lesson 5	Threats, Attack Scenarios, and Countermeasure <i>Case Study</i> <i>Mumbai Attack, 2008</i>
Lesson 6	Intelligence, Counterintelligence, and Information Sharing
Lesson 7	Design and Evaluation of Physical Protection Systems
Lesson 8	Design and Evaluation of Protection Systems <i>Case Study</i> <i>Fort Hood Shootings, 2009</i>
Lesson 9	Protect and Maintain Telecommunications & Information Technology <i>Case Study</i> <i>Internet Attacks, 2011</i>
Lesson 10	International Critical Infrastructure Systems and Dependency
Lesson 11	Science and Technology
Lesson 12	Future Challenges to the Critical Infrastructure
Lesson 13	Future Challenges to the Critical Infrastructure <i>Case Study</i> <i>Japan's Catastrophic Disaster: Earthquake, Tsunami, and Nuclear Energy</i>
Lesson 14	Student Term Paper Presentations
Lesson 15	Student Term Paper Presentations

*Student Group Case Study Presentations will be from open sources only

COURSE OUTLINE

LESSON 1: OVERVIEW OF NATIONAL SECURITY AND DEPARTMENT OF HOMELAND SECURITY FRAMEWORKS

1. Lesson Goals/Objectives:

- Define course requirements and expectations
- Differentiate between national defense and homeland security and understand how they complement one another
- Identify key national security strategies in protecting the homeland
- Contrast pre- and post-9/11 national security issues
- Examine the current organizational structure of DHS
- Understand how to navigate the DHS CIKR Resource Center Web site
- Identify four issues in the article *The Response of People to Terrorism* that should be of concern to the critical infrastructure community

2. Discussion Topics:

- How do the terms “national security” and “homeland security” differ?
- Identify key national security strategies for the protection of critical infrastructure and enhancing its resilience.
- How many critical infrastructure sectors are interdependent?
- What role should science and technology have in countering terrorism?
- If the words “countering terrorism” were replaced with “all-hazards approach,” what are the implications?

3. Required Reading:

National Security Strategy, May 2010 [review only]

<http://www.whitehouse.gov/>.

National Infrastructure Protection Plan: Partnering to enhance protection and resiliency, 2009,

http://www.dhs.gov/files/programs/editorial_0827.shtm.

Homeland Security Critical Infrastructure,

<http://www.dhs.gov/files/programs/critical.shtm>.

Critical Foundations: Protecting America’s Infrastructures,

<http://www.fas.org/sgp/library/pccip.pdf>.

Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, National Research Council, Chapter 9: *The Response of People to Terrorism*, 2002.

4. Activities:

- Small discussion groups will identify five pre- and five post-9/11 critical infrastructures issues and present their findings to the class.

- DVD: *The World Trade Center (WTC): The First 24 Hours*

LESSON 2 & 3 TOPIC: CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE

1. Lesson Goals/Objectives:

- Evaluate how the definition of terrorism shapes U.S. policy toward critical infrastructure
- Define the terms “critical infrastructure protection” and “resilience”
- Describe the national strategies for protecting the critical infrastructure
- Highlight the differences between vulnerability, threat, consequence, and risk assessment
- Explain the issues in policy implementation to protect the critical infrastructure
- Define the differences in protection and resilience strategies between a fixed and mobile critical infrastructure system
- Identify the role of the National Response Framework (NRF) in critical infrastructure prevention, impact mitigation, and emergency response

2. Discussion Topics:

- Identify four issues in the article *The Response of People to Terrorism* that should be of concern to the critical infrastructure community.
- Evaluate key considerations between the protection strategies for fixed and mobile infrastructure assets.
- What are the principal challenges faced in protecting the Nation’s critical infrastructure?
- How many critical infrastructure sectors are interdependent?
- Analyze three issues of concern with complex and interdependent critical infrastructure systems and sectors.
- Define the importance of critical infrastructure resilience.
- Explain the role science and technology should play in prevention, mitigation, and response to critical infrastructure systems.

2. Required Reading:

The 9/11 Commission Report, Chapter 2: *The Foundation of the New Terrorism*.

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.

National Infrastructure Protection Plan: Partnering to enhance protection and resiliency, 2009 [review only].

Mary Lynn Garcia, *The Design and Evaluation of Physical Protection Systems*, Chapter 15 — Risk Assessment (2nd edition, 2010).

Making the Nation Safer: The Role of Science and Technology in Countering Terrorism

- Chapter 8: City and Fixed Infrastructure
- Chapter 10: Complex and Interdependent Systems

National Response Framework (NRF), Homeland Security, January 2008.
Organizational Resilience: Security, Preparedness, and Community Management Systems — Requirements with Guidance for Use, ASIS SPC, 1-2009, ASIS International,
<http://www.asisonline.org/> [review only].

Critical Infrastructure Resilience Final Report and Recommendations, National Infrastructure Advisory Council, [review only],
http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

3. Activity:

- Learners will navigate the DHS Web site responding to questions from the instructor concerning the location of specific topics.

LESSON 4: NATURAL DISASTERS, THREATS, ATTACK SCENARIOS, AND COUNTERMEASURES

1. Learning Goals/Objectives:

- Contrast how prevention, mitigation, and response differ between a natural and manmade threat
- Define the term “threat shifting” as used in the *2010 DHS Risk Lexicon*
- Describe the National Planning Scenarios
- Explain why the conduct and use of a risk assessment by government and industry may differ

2. Discussion Topics:

- The term “threat” is used in many different contexts. Analyze the meaning of “threat” as it applies to an all-hazards approach.
- Should unintentional industrial accidents be considered threats under an all-hazards approach?
- What are the similarities between a natural and man-made threat?
- What is the meaning of the term “technological threat”?
- How are consequences determined when evaluating a natural disaster and man-made event?
- How does “new terrorism” differ from terrorism previous to the 9/11 attacks?
- Explain how and why terrorism tactics, techniques, and procedures are continually evolving? What impact does this have on preventing, mitigating, and responding to attack scenarios?

3. Required Reading:

The 9/11 Commission Report

- Chapter 2: The Foundation of the New Terrorism
- Chapter 3: Counter Terrorism Evolves
- Chapter 6: From Threat to Threat
- Chapter 7: The Attack Looms

4. Activities:

- Presentation of case study
- Case Studies
 - *Hurricane Katrina, 2005-Challenges: Infrastructure and Assessments*

LESSON 5: THREATS, ATTACK SCENARIOS, AND COUNTERMEASURES

1. Learning Goals/Objectives:

- Highlight the differences between a vulnerability and risk assessment
- Explain how critical assets, threats, and consequences are used to evaluate risk.
- Define how risk is managed
- Identify the three physical protection functions
- Compare the different types of countermeasures

2. Discussion Topics:

- Does a facility characterization include supporting missions?
- How would you define countermeasures?
- How does the threat drive the establishment of countermeasures?
- From whose perspective is target identification addressed? How are targets selected (e.g., what criteria are used and why)?
- What key elements are evaluated during the analysis and evaluation phase of the design and evaluation of physical protection?
- In addition to the physical protection systems, what other systemic issues must be considered?
- Threat shifting is the response of adversaries to perceived countermeasures or obstructions in which the adversaries change some characteristic of their intent to do harm in order to avoid or overcome the countermeasure or obstacle (DHS Risk Lexicon, 2010, p. 37). How does threat shifting increase or decrease risk?

3. Required Reading:

Mary Lynn Garcia, *The Design and Evaluation of Physical Protection Systems*, (2nd edition, 2010).

- Chapter 2: Facility Characterization
- Chapter 3: Threat Definitions
- Chapter 4: Target Identification
- Chapter 13: Analysis and Evaluation

National Terrorist Advisory System (NTAS) [review only],

http://www.dhs.gov/files/programs/Copy_of_press_release_0046.shtm.

4. Activities:

- Presentation of case study
- Case Study
 - *Mumbai Attacks, 2008*

Note: A balanced approach is critical to identify effective countermeasures based on level and severity of human and manmade threats (e.g., all hazards) along with a detailed site characterization that provides senior management decision options. Politics from many levels will influence the risk assessment process.

LESSON 6: INTELLIGENCE, COUNTERINTELLIGENCE, AND INFORMATION SHARING

1. Learning Goals/Objectives:

- Identify members of the national intelligence and community
- Explain the difference between information and intelligence
- Define the role of the intelligence community in supporting DHS
- Identify how community involvement is related to countering threats against critical infrastructure systems
- Identify the products Homeland Security Operations Center (HSOC) can provide to help deter, detect, and prevent terrorist acts
- Explain the term “information sharing” as it pertains to the 18 sectors
- Define “Operation SAFEGUARD” as used by the New York Police Department

2. Discussion Topics:

- How should the community become involved in protecting critical infrastructure?
- What is the National Joint Terrorist Task Force (NJTTF) and what does it mean when it is described as “the point of fusion”?
- Describe information-sharing partnerships with the private sector. What barriers are there to sharing information?
- By what criterion does a private business base their decision to become involved with an information-sharing relationship with the public sector?
- Information sharing is a key element of our national strategy in counterterrorism and homeland security. What are the pros and cons of information sharing?
- The Nationwide Suspicious Activity Report (SAR) Initiative was established to provide a unified process for reporting, tracking, and accessing information that may forewarn of a future terrorist attack. The long-term goal is for Federal, State, local, tribal, and territorial law enforcement organizations, as well as private sector entities, to participate in the National SAR initiative. What type of information is needed from SAR to protect critical infrastructure sectors?
- How does Operation SAFEGUARD apply to the critical infrastructure sectors?

3. Required Reading:

Office of the Director of National Intelligence (ODNI) [review only],
<http://www.dni.gov/>.

Office of the Director of National Intelligence — ODNI Fact Sheet,
http://www.dni.gov/content/ODNI%20Fact%20Sheet_Oct2010.pdf.

Homeland Security: *Protecting, Analyzing & Sharing Information* [review only],
<http://www.dhs.gov/files/programs/sharing-information.shtm>.

United States Intelligence Community Information Sharing Strategy, February 2008,
http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf.

The CIP Report, May 2010 Information Sharing,

http://cip.gmu.edu/index.php?option=com_k2&view=item&id=140:the-cip-report&Itemid=74.

National Suspicious Activity Reporting (SAR) Initiative (NSI), <http://nsi.ncirc.gov/>.

Transportation Sector Information Sharing, <http://www.ise.gov/sharing-private-sector>.

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

Note: Not all customers or agencies use the same criteria for defining classification categories or levels of sensitivity. Consult Federal, State, local, tribal, and territorial guidance for classified and other sensitive official materials.

LESSONS 7 & 8: DESIGN AND EVALUATION OF PHYSICAL PROTECTION SYSTEMS

1. Learning Goals/Objectives:

- Evaluate the necessary elements of a physical protection system
- Explain how response is integrated into the protection of critical infrastructure
- Create a countermeasure plan, given a schematic of a critical infrastructure asset
- Discuss the role of private security in infrastructure protection

2. Discussion Topics:

- Physical protection technology and hardware are elements of a robust physical protection system. What other elements are required to have an integrated physical protection system?
- A key element in designing and implementing a physical protection system is senior management buy-in. In the private sector, the bottom-line is always profitability and return-on-investment. How would you persuade senior management that a new or upgraded physical protection system is cost effective?
- Numerous vendors provide physical security systems, some reputable and some not so reputable. When evaluating the purchase of or upgrading to a physical protection system, what criteria should be used in evaluating the trustworthiness of a vendor?
- A postulate threat based scenario is used during planning to prevent, mitigate, and responded to hypothetical scenarios. What mechanism would you need in place to maintain updated information on emerging threats?
- A common threat scenario is for an adversary to be disguised as a legitimate vendor. What policies and procedures would you need in place to verify a vendor's identity?
- Exterior and interior intrusion security protection systems are used to provide defense-in-depth and detection. Describe the criteria used in the decision process for selecting an exterior or interior system.

3. Required Reading:

Mary Lynn Garcia, *The Design and Evaluation of Physical Protection Systems*, (2nd edition, 2010).

- Chapter 1: Design and Evaluation of Physical Protection Systems
- Chapter 5: Physical Protection Systems
- Chapter 6: Exterior Intrusion Systems
- Chapter 7: Interior Intrusion Systems
- Chapter 10: Entry Control

4. Activities

- Presentation of a case study
- Create a countermeasure plan
- Case Study:
 - *Fort Hood Shootings, 2009*

Note: The majority of critical infrastructure is owned or operated by the private sector. Uniqueness of each site's defined risk and the integration of components systems, including response (e.g., contract security, proprietary security, law enforcement, emergency management, Federal, State, local, tribal, and territorial resources) must be integrated into the overall protection strategy — prevent, mitigate, and respond.

LESSON 9: PROTECT AND MAINTAIN TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

1. Learning Objectives:

- Define cybersecurity, cybercrime, and cyber-terrorism
- List five possible critical infrastructure cyber vulnerabilities
- Evaluate the emerging advanced persistent cyber threat against critical infrastructure
- Identify the strategic goal of DHS in combating cyber threats
- Understand the potential effectiveness of a combined cyber and physical attack against critical infrastructure

2. Discussion Topics:

- “The convergence of technological and socio-political trends indeed suggests that cyber-terrorism may be the wave of the future” (from Rand Report: *Cyber-terrorism The Threat of the Future?*). Assuming this is a true statement, what are the strategic implications in the protection and resilience of critical infrastructure?
- *National Strategy to Secure Cyberspace* provides a framework for protecting the infrastructure and is essential to our economy, security, and way of life. It is an implementing component of the *National Strategy for Homeland Security* and is complemented by a *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Explain why the cyber threat is a seminal issue in protecting critical infrastructure systems.
- The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all. The private sector is hesitant to report such attacks. Why is this? What can be done to increase reporting?
- A key ingredient of the Advanced Persistent Threat (APT) is the abuse and compromise of “trusted connections.” What does this mean? How can this threat be countered?
- In *Cyber-terrorism: The Threat of the Future?*, do these emerging threats impact critical infrastructure sectors differently? If so how?

3. Required Reading:

Department of Homeland Security Strategic Plan 2008, [search for cyber security] [review only].

http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf.

National Strategy to Secure Cyberspace [review only],

http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

DHS Office of Cyber Security and Communications, [review only],

http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm.

Statement of General Victor E. Renuart, Jr. USAF Commander United States Northern Command and North American Aerospace Defense Command Before the Senate Armed

Services Service Committee 11 March 2010,
<http://www.rand.org/content/dam/rand/www/external/nsrd/DoD-CBRNE-Panel/panel/meetings/20100317/D-4-Statement-of-Commander-United-States-Northern-Command.pdf>.

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

Cyberspace Policy Review, 2009,
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Advanced Persistent Threats (APT), <http://www.damballa.com/knowledge/advanced-persistent-threats.php>.

George Mason University Center for Infrastructure Protection and Homeland Security, *IT Overview*,
http://cip.gmu.edu/index.php?option=com_k2&view=item&id=58:overview&Itemid=70.

4. Activities

- Presentation of case study
- Case Study:
 - *Internet Attacks, 2011*

LESSON 10: INTERNATIONAL CRITICAL INFRASTRUCTURE SYSTEMS AND DEPENDENCY

1. Learning Objectives:

- Understand national and international security implications where critical infrastructure shares international boundaries
- Identify countries who do not share our borders and the implications on critical infrastructure and resilience
- Name at least four critical infrastructure sectors that cross the U.S. Canada and Mexico borders
- Compare national and international issues in critical infrastructure
- Understand the complexity and interdependency of critical infrastructure in a global economy

2. Discussion Topics:

- What are U.S. critical infrastructure security implications from countries who do not share our borders?
 - Identify possible disruption of manufacturing and supply?
 - What are the pros and cons in information sharing?
 - What can we learn from these countries?
- As globalization, internationalism, environmental concerns (e.g., global warming), and limited resources become more evident in the 21st century, how will these factors play out in protecting our Nation's critical infrastructure?
- The world is becoming more complex and interdependent. New technologies are emerging, boundaries are disappearing, and social media is used to topple governments. The Internet has changed economics, culture, and politics. As these changes accelerate, what impact will they have on national and international critical infrastructure systems?

3. Required Reading:

International Issues for CI/KR Protection,

http://www.dhs.gov/xlibrary/assets/nipp_international.pdf.

Critical Foreign Dependencies Initiative, (CFDI),

http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (p. 40).

The CIP Report, George Mason University Center for Infrastructure Protection and Homeland Security, www.cipp.gmu.edu.

- *June 2010 International CIP*
Afghanistan Infrastructure, page 9
Infrastructure Regulation, page 10
- *July 2009 International CIP*
Australian Infrastructure, page 2
Italian Infrastructure Protection, page 5
- *June 2008 International CIP*

Australian Resilience Planning, page 4
European Union CIP, page 9

4. Activity:

- Divide learners into groups to identify critical infrastructure protection international interdependencies. Assign a different country to each; group leader presents findings.

LESSON 11: SCIENCE AND TECHNOLOGY

1. Learning Objectives:

- Explain how DHS provides knowledge products and innovative technology solutions for homeland security
- Identify the kinds of research DHS is conducting to address critical homeland security needs
- Identify how DHS transitions and commercializes the results of its technology research for use by the critical infrastructure community
- Understand the advantages and disadvantages of technology in critical infrastructure systems

2. Discussion Topics:

- Renewed focus on counterterrorism (CT) and homeland security has served as a catalyst to promote the increased use of technology. What are some of the advantages and disadvantages within a democratic society expanding the use of these technologies?
- Where do you see gaps in CT and homeland security capabilities that might be filled by new technology?
- Explain the role science and technology should play in the prevention, mitigation, and response to critical infrastructure systems.
- Use of the latest security technology is touted as the "solution." What criteria should be used before investments are made in state-of-the-art security technology?

3. Required Reading:

Making the Nation Safer: The Role of Science and Technology in Countering Terrorism

- Chapter 10: Complex and Interdependent Systems

The 9/11 Commission Report

- Chapter 10: War Time
- Chapter 11: Foresight—And Hindsight

Department of Homeland Security's Science and Technology Directorate — Tech Solutions Program [review only],

http://www.dhs.gov/xfrstresp/training/gc_1174057429200.shtm.

Long-Term Effects of Law Enforcement's Post-9/11 Focus on Counterterrorism and Homeland Security Summary Report, Rand Corporation,

http://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG1031.sum.pdf

LESSON 12 & 13: FUTURE CHALLENGES TO CRITICAL INFRASTRUCTURE

- Threats
 - Radicalization
 - Female Suicide Bomber
 - Homegrown Terrorist
- Cyberterrorism and the Advanced Persistent Threats (APT)
- NIPP and Sector-Specific Plans (SSP) Continuous Improvement

1. Learning Objectives:

- Identify emerging threats and their impact on critical infrastructure systems
- Understand how the advanced persistent threats could impact critical infrastructure systems
- Explain the rationale for continuous improvement of NIPP and SSPs

2. Discussion Topics:

- In July 2010, at Secretary Janet Napolitano's direction, DHS launched a national "If You See Something, Say Something™" public awareness campaign.
 - What criteria would you use to evaluate the effectiveness of such a public awareness campaign?
 - What are some of the advantages and disadvantages of these programs?
 - Can you identify similar programs in your jurisdiction?
 - What role does culture play (e.g., Israel vs. U.S.)
- As new threats emerge and the adversary adapts seemingly overnight to introduce new attack scenarios (e.g., liquid explosives, selecting unknowing individuals as suicide bombers, secreting explosives in body cavities, etc.), it has become more difficult to neutralize these threats. Most critical infrastructure systems are at fixed physical locations, i.e., hard targets. An emerging trend is to attack mobile or soft targets (e.g., hotels, railways, subways, crowds, etc.). As these trends emerge, how flexible do we need to be in order to get ahead of the threat? How would this be accomplished?
- In a democratic society "freedom" and "security" are always at odds because security implies restrictions. Seeking to balance these two competing goals makes for difficult choices. Are individual rights paramount or do the means justify the end in preventing another 9/11?
 - What criteria would you use in achieving equilibrium between these two competing goals?
 - How would you quantify the costs if one goal outweighed the other by a very large sum?

3. Required Reading:

U.S. Counterterrorism Strategy Must Address Ideological and Political Factors at the Global and Local Levels,

http://www.rand.org/pubs/research_briefs/RB202/index1.html.

Homeland Security Sector-Specific Plans [review only],
http://www.dhs.gov/files/programs/gc_1179866197607.shtm.

J. McNeill and James Carafano, Executive Summary Backgrounder, *Terrorist Watch: 23 Plots Since 9/11*, Published by The Heritage Foundation, (2 July 2009), Retrieved from
http://s3.amazonaws.com/thf_media/2009/pdf/bg2294.pdf.

B. Jenkins, *Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States since September 11, 2001*, RAND, (2010), Retrieved from
http://www.rand.org/pubs/occasional_papers/OP292/.

A. Speckhard and K. Akhmedova, "Black Widows: The Chechen Female Suicide Terrorists," In Yoram Schweitzer ed., *Female Suicide Terrorists: Dying for Equality?* Jaffe Center Publication, Tel Aviv, Israel, (2006) [review only],
<http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0C54E3B3-1E9C-BE1E-2C24-A6A8C7060233&lng=en&id=91164>.

"If You See Something, Say Something™" Campaign DHS
<http://www.dhs.gov/files/reportincidents/see-something-say-something.shtm>.

4. Recommended Reading:

Barabási Albert-László, *Linked: How Everything Is Connected to Everything Else and What It Means*.

5. Activities:

- Presentation of case study
- Case Study:
 - *Japan's Catastrophic Disaster: Earthquake, Tsunami, and Nuclear Energy*

WEEK 14 & 15: STUDENT TERM PAPER PRESENTATIONS

1. Learning Objectives:

- Understand how well he or she met the requirements stated in Section XII of this syllabus

2. Discussion Topics:

- Term Paper Presentation

3. Activities:

- Learners will present a short fifteen minute overview of their term paper
- Each presenter will be prepared to answer relevant questions on their term paper
- Instructor will provide constructive feedback to each presenter

CASE STUDY GUIDANCE

1. Purpose: Real-world events provide a rich learning environment. Case studies from historical events and natural disasters will be used to highlight course learning objectives.

2. Goal: To provide a student-centered learning environment where real-world events can be used as a vehicle linking the academic classroom with actual events. Highlighting issues where policy, procedures, and classroom solutions may not have considered the dynamic and multi-facet issues confronting critical infrastructure from malevolent and natural disasters, possibly across sectors and international implications.

3. Action:

- Small collaborative groups will be assigned a topic to research, write a report, and present findings to the class. Topics are:
 - *Hurricane Katrina, 2005-Challenges: Infrastructure and Assessments*
 - *Mumbai Attack, 2008*
 - *Fort Hood Shootings, 2009*
 - *Internet Attacks, 2011*
 - *Japan's Catastrophic Disaster: Earthquake, Tsunami, and Nuclear Energy*
- Each collaborative group will pick a leader and spokesperson.
- Research will be conducted on the assigned topic. ONLY open sources will be used.
- Presentation dates coincide with the lessons listed in **Course Topics** of this syllabus.
- Each group will have thirty-minute to present their report.
- The leader or designee will lead a seminar discussion on the topic.
- An electronic copy of slide notes will be provided each student two days prior to the presentation.

4. References:

Review sector-specific plans:

http://www.dhs.gov/files/programs/gc_1179866197607.shtm.

National Preparedness Guidelines (Review Types of National Planning Scenarios),

http://www.dhs.gov/xlibrary/assets/National_Preparedness_Guidelines.pdf.

5. Focus:

- Provide an overview of the assigned case study; identify sector(s) involved and issues related to critical infrastructure resilience based on course learning objectives.
- Additional guidance will be provided the first class.