**Course Number: XXXX**

**Course: Information Sharing for 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:**

This graduate course provides an overview of information sharing within the national security/homeland security enterprise with a focus on the information sharing necessary to protect and make the Nation’s critical infrastructure more resilient. This is a multi-faceted course that will expose learners to complex public-private sector policies, plans, partnerships, processes, procedures, systems, and technologies for information sharing. The course is designed to promote subject-matter understanding, critical analysis of issues, and insight into senior leader decision-making in both the public and private sectors. It also includes a practical examination of stakeholder interaction through an interactive tabletop (or, alternatively, computer lab) exercise, the development and sharing of a threat-warning product, a research paper, and oral presentation. The overall goal is for learners to gain insights into how the sharing and fusion of information can lead to timely and actionable products that, in turn, will enable private sector owners and operators to become better prepared and be better able to protect the Nation’s critical infrastructure. Finally, the course will demonstrate how information sharing can serve as an enabler to foster a partnership-focused networked protection and resilience regime.

**Credits Conferred:** 3

**PREREQUISITE:**  Introduction to Critical Infrastructure Security and Resilience

**Learner Outcomes/Objectives (As Mapped Against Department of Homeland Security Critical Infrastructure Core Competencies):**

This course is designed to enable learners to:

1. **Identify the authorities, roles, responsibilities, and capacities of key critical infrastructure public and private sector stakeholders regarding homeland security information sharing:**

* Federal, State, tribal, territorial, regional, local, private sector, and international
* Touch points, barriers, and flash points
* Laws, regulations, incentives, and motivations

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

* Federal, State, tribal, territorial, regional, local, private sector, and international collaboration, coordination, and communication
* CI data collection, warehousing, and protection
* Connecting the “Four Ps”: People, processes, products, and pipes
* Systems challenges and opportunities

**3. Evaluate the critical infrastructure** **Partnership in Action: National critical infrastructure information sharing foundations, frameworks, and selected sector procedures**

* Anthrax attacks through the U.S. postal system
* National Terrorism Advisory System (formerly Homeland Security Advisory System) Alerts (e.g., Aviation Subsector)
* London Transit Bombings
* Christmas Day Bomb Threat
* Aviation Cargo Parcel Bombs
* Boston Marathon Bombing
* Terrorist Surveillance of a Nuclear Power Plant (exercise)

**Delivery Method/Course Requirements:**

Course delivery will be through directed readings, class participation, information sharing product preparation, research paper, information sharing exercise, and class oral presentation. This is a graduate level course. The learner will gain, in an independent manner, a body of knowledge pertaining to critical infrastructure security and resilience and an ability to communicate his/her understanding and assessment of that knowledge to fellow participants and faculty via discussions and written papers. Learners are expected to familiarize themselves with the assigned topic and readings before class and should be prepared to discuss and debate them critically.

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 cell phones should be turned off before class begins.

**Grading**

Class Participation 20%

Information Sharing Product 15%

Research Paper 35%

Research Paper Presentation 10%

Information Sharing Case Study 20%

**Activities, Exercise And Research Projects:**

1. **Information Sharing Product Preparation (15%)**

Each learner will prepare a threat-warning product for sharing. Details are given in Lesson 9.

1. **Research Paper/Oral Presentation: (45%)**

Each learner will prepare a 15-20 page research paper on a critical infrastructure information sharing issue of their choice (National, regional, State, local, 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 the selections). 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 information sharing policies, procedures, or mechanisms. The recommendations section should clearly describe the rationale for the policy options of choice.

One area that is particularly fertile ground for a research paper is to identify an information sharing barrier, explain why and how it is a barrier, and then propose solutions to overcome it. A partial list of possible information barriers includes:

* Lack of nationwide awareness of the existence of the public-private partnership for critical infrastructure, how to participate in it, including its information sharing mechanisms
* Lack of a national integrated communications-collaboration-information system that operates at all required classification levels
* The process required for critical infrastructure owners and operators to obtain and maintain a security clearance
* Inability of critical infrastructure owners and operators to make the business case for taking the time to participate in information sharing within their critical infrastructure sector and/or with the government
* Insufficient Federal government resources to fully support Critical Infrastructure Information Sharing Working Groups, to include staffing, subject-matter experts, and compensation for time and travel
* Inadequate attention paid to the front end of the information sharing lifecycle, namely to the definition of critical infrastructure information and intelligence needs and requirements
* Lack of U.S. Department of Homeland Security (DHS) statutory authority to declassify or downgrade information classified by other Federal agencies in order to share it more broadly with critical infrastructure owners and operators
* Lack of sufficient credible indications and warnings that can be responsibly shared
* Lack of training for owner and operator staff and decision-makers about how to deal with marginally credible threat information
* Fears of liability that may accompany advance knowledge of risks
* Lack of proactive risk information exchanges short of credible threat warnings, such as identification of shared risks and collaboration on how to manage them

Each learner will present a **summary** of his/her research topic (no more than 6-10 minutes in length) to the class during Lesson 15. The presentation format will mirror that of the research paper. **Research papers will be submitted either in person or electronically on the day of the learner’s oral classroom presentation.** 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.**

**3. Information Sharing Case Study (20%)**

Learners will apply critical infrastructure security and resilience knowledge and skills to a case study of the 2001 Howard Street Tunnel Fire. Prior to class, learners should read the specified case narrative and be prepared to engage in critical analysis. Subsequent to the in-class discussion and evaluation, learners will complete a 2-3 page reflection paper chronicling his/her experience and lessons learned. **Reflection papers will be submitted at the beginning of the next class.**

**4. Expectations for Participation (20%)**

Participation includes coming to class prepared and participating in class discussion.

**Incorporation of Feedback**:

The course instructor will provide multiple opportunities for learners to provide constructive feedback over the period of the course. These may be in the form of group sessions or one-on-one sessions with the instructor. Learners will be afforded the opportunity to complete in-class evaluations following the critical infrastructure information sharing case study, as well as 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 course research paper, oral presentation, and information sharing product paper.

**Course Textbooks:**

The following textbook is identified as a primary textbook for the course. The textbook will be supplemented by additional readings for each lesson either accessible on-line (with website addresses provided in the lesson description sections that follows below) or provided by the instructor.

[Bullock](http://www.amazon.com/s/ref=ntt_athr_dp_sr_1?_encoding=UTF8&sort=relevancerank&search-alias=books&field-author=Jane%20Bullock), Jane, [Haddow](http://www.amazon.com/s/ref=ntt_athr_dp_sr_2?_encoding=UTF8&sort=relevancerank&search-alias=books&field-author=George%20Haddow), George, [Coppola](http://www.amazon.com/s/ref=ntt_athr_dp_sr_3?_encoding=UTF8&sort=relevancerank&search-alias=books&field-author=Damon%20P.%20Coppola), Damon P., [and Yeletaysi](http://www.amazon.com/s/ref=ntt_athr_dp_sr_4?_encoding=UTF8&sort=relevancerank&search-alias=books&field-author=Sarp%20Yeletaysi), Sarp. *Introduction to Homeland Security, Fourth Edition: Principles of All-Hazards Response*. Burlington, MA: Butterworth-Heinemann, 2012.

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

**Course Outline**

**Lesson 1 Topic: The Need For Information Sharing For Critical Infrastructure Security And Resilience**

**1. Lesson Goals/Objectives:**

* Discuss the course scope/content, administrative requirements, instructional methodology, evaluation criteria, and feedback processes.
* Explain the evolution of critical infrastructure security and resilience partnerships and information sharing (and related lexicon) as a national policy focus areas.
* Analyze why government-private partnership and information sharing arose out of the Oklahoma City (1995) and September 11 (2001) attacks.
* Analyze the differences in the needs for information sharing within the Intelligence Community (IC); between the IC and other Federal agencies (including DHS); and between Federal agencies and State, local, tribal, and territorial governments, as well as regional, private sector, and international partners.
* Explain the differences and similarities in the kinds of information that need to be shared prior to, during, and after a major natural disaster, a terrorist attack on the homeland, and other man-made events.
* Explain the need for routine risk information sharing to support government-private sector planning and resource investment for critical infrastructure security and resilience.
* Explain the fundamental barriers to partnerships and information sharing within the critical infrastructure and resilience mission area.

**2. Discussion Topics:**

* What were the barriers to information sharing between elements of the IC and the Law Enforcement community (e.g., FBI) pre-9/11?
* Which barriers were legislative/ regulatory and which were institutional/cultural pre-9/11?
* How would you characterize the differences — with respect to ease, speed, and content — between information sharing among the following partners: the IC and other Federal agencies, including DHS; between DHS and Federal, State, and local Governments; and between DHS and private sector partners?
* What are the barriers to sharing Law Enforcement Sensitive (LES) and classified information with the private sector today? Can these barriers be overcome?
* How can *unclassified* information be used to protect critical infrastructure in advance of a terrorist attack or major natural disaster?
* How can *classified* information be used to protect critical infrastructure in advance of a terrorist attack or major natural disaster?
* What did the WikiLeaks event during December 2010 illustrate regarding controls for handling sensitive and classified information?
* Give an example, real or hypothesized, concerning how government and industry might share risk information for purposes of planning critical infrastructure security and resilience.

1. **Required Reading:**

Textbook: Chapters 1-2

Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2006). http://www.intelligence.senate.gov/laws/pl11053.pdf.

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

The 9/11 Commission. *The 9/11 Commission Report*. 2004.chap. 3, 8. <http://govinfo.library.unt.edu/911/report/index.htm>.

USA PATRIOT Act of 2001,Pub. L. No. 107-56, 115 Stat. 272, (2001). <http://fl1.findlaw.com/news.findlaw.com/wp/docs/terrorism/patriotact.pdf>.

**4. Additional Recommended Reading:**

Hoffman, David. *The Oklahoma City Bombing and the Politics of Terror*. 1998.

<http://www.jrbooksonline.com/PDF_Books_added2009-4/ocbpt.pdf>.

*The Need to Know: Information Sharing Lessons For Disaster Response*: *Hearing Before the Comm. on Government Reform*, 109 Cong.143 (2006).

<http://www.fas.org/sgp/congress/2006/infoshare.html>.

The White House, *The Federal Response to Hurricane Katrina - Lessons Learned*. 2006. <http://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned/>.

**Lesson 2 Topic: Legislative And Executive Policy Mandates For Information Sharing**

**1. Lesson Goals/Objectives:**

* Explain how the various acts of legislation and Executive Orders and policies governing government-private sector partnerships and information sharing.
* Describe the foundation provided by the 9/11 Commission Report for much of the policy put in place over the past decade in this area.
* Explain the concepts and functions associated with the Information Sharing Environment (ISE) created by the Intelligence Reform and Terrorism Reduction Act (IRTRA) of 2004, including the ISE private sector component.
* Recognize Describe the role of the DHS/Office of Infrastructure Protection as Federal lead for integration of the private sector into the ISE.

1. **Discussion Topics:**

* Why was there a need to enact IRTRA subsequent to the Homeland Security Act of 2002? What new authorities were provided and for whom did it provide them?
* When DHS was reorganized after the Second Stage Review, where was the responsibility placed for sharing threat information with the critical infrastructure sectors?
* How do the referenced acts of legislation, Executive Orders, policies, and strategies address the matter of sharing information between government and the private sector, and vice versa? Do any of the legislative or executive mandates direct or request the private sector to share information?
* What is the significance of making the private sector an official component of the ISE? How does it affect the Government – private sector relationship?
* How do the 2014 Quadrennial Homeland Security Review and DHS Bottom-Up Review address partnering and sharing information for critical infrastructure and resilience?
* Taken collectively, do all of the authorities and mandates referred to above provide an adequate basis for a robust information sharing environment? Are any additional authorities needed?

1. **Required Reading:**

Textbook: Chapters 3-4

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

U.S. Department of Homeland Security. *Bottom-Up Review*. 2010.

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

U.S. Gov’t Accountability Office GAO-08-492, *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress,* (2008), http://www.gpo.gov/fdsys/pkg/GAOREPORTS-GAO-08-492/content-detail.html.

Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002). <http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf>.

Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, 118 Stat. 3638. <http://www.nctc.gov/docs/pl108_458.pdf>.

The White House. *National Strategy for Information Sharing*. 2007.

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

ISE. ”Sharing with the Private Sector.” Accessed July 1, 2014. http://www.ise.gov/sharing-private-sector.

Information Sharing Governance Board. *DHS Strategy for Information Sharing*.

2008. <http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf>.

The White House. *Guidelines and Requirements in Support of the Information Sharing Environment*. 2005. <http://www.fas.org/sgp/news/2005/12/wh121605-memo.html>.

The 9/11 Commission. *The 9/11 Commission Report*. 2004. chap. 13.<http://govinfo.library.unt.edu/911/report/index.htm>.

1. **Additional Recommended Reading:**

Best Jr., Richard A. Cong. Research Serv., RL33873. *Sharing Law Enforcement and Intelligence Information.* 2007. <http://www.fas.org/sgp/crs/intel/RL33873.pdf>.

IT Law Wiki. “Information Sharing Environment.” Accessed June 19, 2014.

<http://itlaw.wikia.com/wiki/Information_Sharing_Environment>.

Paul, Kshemendra N. *InformationSharing Environment: Annual Report to Congress*. 2010.

http://www.fas.org/irp/agency/ise/2010report.pdfPiette, D.C. and Radack, J. “Piercing the ‘Historical Mists’: The People and Events Behind

the Passage of FISA and the Creation of the ‘Wall’.” *Stanford Law and Policy Review*

2006: 261.

Information Sharing Environment.

*Information Sharing Environment Implementation Plan.* 2006.

<http://www.fas.org/irp/agency/ise/plan1106.pdf>.

The White House. *National Security Strategy*.2010.

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

**Lesson 3 Topic: Foundations For Successful Information Sharing**

**1. Lesson Goals/Objectives:**

* Evaluate the following principles or “best practices” that comprise the necessary foundation for a successful information sharing community:
* Fostering trusted relationships
* Obtaining management support
* Establishing mutual benefits
* Defining effective communications and workflow processes
* Filtering information for relevance to decision makers
* Training and retaining staff with appropriate skills

**2. Discussion Topics:**

* What is an information sharing community?
* Why is developing one-on-one relationships within the information sharing community so fundamental to enabling the sharing of sensitive information?
* What are the draw backs to ‘personality driven’ information sharing relationships?
* What barriers to the sharing of sensitive information do trusted relationships overcome?
* What venues are available for government and the private sector to develop trusted relationships?
* Why is obtaining management support necessary for initiating and sustaining information sharing?
* What are some of the mutual benefits gained by government and the private sector through information sharing?
* What are some of the most effective communication and workflow processes and practices?
* What kinds of skills do government and the private sector need training on in order to sustain a successful information sharing community?

**3. Required Reading:**

Textbook: Chapters 5-6

Dorner, D. *Logic of Failure: Recognizing and Avoiding Error in Complex Situations*.

Perseus Books: Cambridge, 1996.

Heimer, C.A. “Doing your Job and Helping your Friends: Universal Norms about Obligations to Particular Others in Networks.” In *Networks and Organizations Structure: Form and Action*, edited by N. Nohria and R.G. Eccles. Harvard Business School Press, 1992.

Wohlstetter, R. *Pearl Harbor: Warning and Decision*. Stanford University Press: Stanford, 1962.

**Lesson 4 Topic: Framework For Information Sharing**

**1. Lesson Goals/Objectives:**

* Identify the five-dimensional framework for effective information sharing, including the following key component elements:

### Information Sharing Terminology and Definitions

### Systems Used to Handle or Control Information Dissemination

### Senders and Receivers

### Technology

### Performance Metrics and Feedback Mechanisms

* Explain how each information sharing partner should be both a “sender” and a “receiver” of information,
* Explain the key critical infrastructure and resilience partnership and information sharing nodes and information flows between them as discussed in the NIPP.
* Identify the various methods, processes, and systems that the various critical infrastructure security and resilience partners use to share information with one another.
* Explain the requirement for adopting common information sharing lexicon in the context of critical infrastructure security and resilience.

**2. Discussion Topics:**

* What are some of the most important terms used in discussing information sharing and what do they mean? Is there a common lexicon you can identify that defines these terms? Why or why not?
* What are some of the most commonly used systems for sharing information between the government and industry for purposes of critical infrastructure security and resilience? Why is it important that there be a common set of systems used by all information sharing partners?
* What are some of the systems used to share classified information? Do you think that many private sector individuals have access, or should have access, to them?
* Within the public-private partnership, who are generally the senders and receivers of information? Are there multiple sender roles? Are there multiple receiver roles (e.g., trusted intermediaries)?
* What are some of the technologies currently used to control the dissemination of, or access to, sensitive but unclassified (SBU) information? Why are protection and sharing like the two sides of the same coin?
* How will implementing performance metrics and feedback mechanisms enhance information sharing? For each information sharing partner identified in the objectives above, give one example of a performance metric.

1. **Required Reading:**

Textbook: Chapters 7-8.

U.S. Department of Homeland Security. NIPP 2013, Partnering for Critical Infrastructure Security and Resilience. 2013, pp. 1-4, appendices A-B. <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.

P. Adriaans, P and Benthem, J.V. “Philosophy of Information.” In*Handbook of the Philosophy of Science*, edited by Gabby, Thagard, and Woods. Elsevier, 2008. <http://store.elsevier.com/product.jsp?isbn=9780444517265>.

Barrett, S. and Konsynski, B. “Inter-Organizational Information Sharing.”

*MIS Quarterly* 6 Special Issue (1982): 93-105.

<http://www.jstor.org/stable/248993?seq=1>.

Constant, D., Kiesler, S., and Sproull, L. “What’s Mine is Ours, or Is It? A Study of Attitudes about Information Sharing.” *Information Systems Research* 5(4) (1994): 400-421.

<http://www.cs.cmu.edu/~kiesler/publications/PDFs/Constant1994WhatsMine%20.pdf>.

Correa Da Silva, F.S. and Agusti-Cullell, J. *Information Flow and Knowledge Sharing*.

Elsevier, 2008.

U.S. Department of Homeland Security, *DHS Risk Lexicon: 2010 Edition*. 2010.

<http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>.

Lee, H.L., So, K.C., and Tang, C.S. “The Value of Information Sharing in a Two-Level Supply

Chain.” *Management Science* 46(5) (2000): 626-643.

<http://www.ie.bilkent.edu.tr/~ie572/Papers/Leeetal2.pdf>.

Malone, T.W., Grant, K.R., Turbak, F.A., Brobst, S.A., and Cohen, M.D. “Intelligent

Information-Sharing Systems.” *Communications of the ACM* 30(5) (1987): 390-402.

<http://dspace.mit.edu/bitstream/handle/1721.1/2157/SWP-1850-21289506-CISR-147.pdf;jsessionid=F33D549DA175C8D1BC3D3AD22B43A213?sequence=1>.

**Lesson 5 Topic: Information Sharing Partners**

**1. Lesson Goals/Objectives:**

* Explain the relationships and processes that link the major parties involved in critical infrastructure security and resilience information sharing, including the following pair-wise groupings of partners:
* Federal government - Federal government (includes IC agencies to non- Intelligence Community Federal agencies)
* Federal government – State and local, tribal, and territorial governments
* Federal government – Private Sector (DHS, FBI, Federal Sector Specific Agencies (SSAs) under the NIPP, etc.)
* State and local Government – Private Sector (includes Law Enforcement to Private Sector, Fusion Centers to Private Sector, Emergency Operations Centers to Private Sector)
* Regional Consortia – Private Sector
* Private Sector - Private Sector (includes Information Sharing and Analysis Centers (ISACs) and Trade Associations to their members)
* Describe the key organizations that have formed to facilitate critical infrastructure security and resilience information sharing
* Analyze the nature of the State, local, and regional Fusion Centers in the context of the critical infrastructure security and resilience mission area
* Describe the special challenges associated with sharing information with tribal and territorial communities.

**2. Discussion Topics:**

* For each pair-wise grouping of partners, what are some of the specific organizations involved and what kind of information do they share?
* What role does each of the following organizations play in CISR information sharing?
* Sector Coordinating Councils
* SSAs and Government Coordinating Councils (GCCs)
* State and Local, Tribal and Territorial - Government Coordinating Council (SLTT-GCC)
* Regional Consortia
* Critical Infrastructure Partnership Advisory Council (CIPAC)
* ISACs and the ISAC Council
* State and local Fusion Centers
* Joint Terrorism Task Forces (JTTFs)
* State and local Emergency Operations Centers (EOCs)
* DHS/ Intelligence and Analysis
* DHS/ National Infrastructure Coordination Center (NICC)
* DHS/Regional Protective Security Advisors (PSAs) and Regional Mission Collaboration Staff
* DHS/Federal Emergency Management Agency (FEMA)
* What type of information is needed by critical infrastructure owners and operators to better protect and make their infrastructure more resilient? Who provides this kind of information?
* Why are the Federal government – Private Sector, State and local government – Private Sector, and Federal government – State and local government the most import pair-wise groupings for sharing critical infrastructure security and resilience information?
* What information does the government need from the private sector in order to build its risk management budgets, plans, and policies?
* What do you think of the adequacy of Fusion Center plans to develop critical infrastructure security and resilience capabilities, including information sharing with local critical infrastructure security and resilience owners and operators?
* How can the Federal government overcome the special challenges associated with sharing information with tribal and territorial communities?

**3. Required Reading:**

Textbook: Chapters 9-10

ISAC Council. *A Functional Model for Critical Infrastructure Information Sharing and Analysis*. 2004.

<http://www.isaccouncil.org/images/Information_Sharing_and_Analysis_013104.pdf>.

ISAC Council. *A Policy Framework for the ISAC Community.* 2004.

http://www.isaccouncil.org/images/Policy\_Framework\_for\_ISAC\_Community\_013104.pdf.

U.S. Department of Homeland Security. *State and Local Fusion Centers*. Accessed July 1, 2014.

# <http://www.dhs.gov/files/programs/gc_1156877184684.shtm>.

Department of Justice. [*Critical Infrastructure and Key Resources (CI): Protection Capabilities for Fusion Centers*](http://www.it.ojp.gov/docdownloader.aspx?ddid=1136). 2008. <http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181>.

U.S Gov’t Accountability Office GAO-10-41, *Information Sharing: Federal Agencies Are Sharing Border and Terrorism Information with Local and Tribal Law Enforcement Agencies, but Additional Efforts Are Needed*,(2009),

<http://www.gao.gov/new.items/d1041.pdf>.

# Additional Recommended Reading:

Boin, Arjen and Smith, Denis. "Terrorism and Critical Infrastructures: Implications for Public-Private Crisis Management," *Public Money & Management* 26(5) (2006): 295-304. http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=937085.

U.S. Gov’t Accountability Office GAO-10-895, *Public Transit Security Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach*,(2010), <http://www.gao.gov/new.items/d10895.pdf>.

Kunreuther, Howard. “Interdependent Disaster Risks: The Need for Public-Private Partnerships.” In *Building Safer Cities: The Future of Disaster Risk*,edited by Alcira Kreimer,MargaretArnold and Anne Carlin, 83-87. Washington, DC: International Bank for Reconstruction and Development, 2003. <http://www.bvsde.paho.org/bvsacd/cd46/cap6-interde.pdf>.

**5. Research Paper Topics Due**

Turn in the proposed research paper topic at the beginning of class per the instructions at the beginning of the syllabus.

**Lesson 6 Topic: Public-Private Partnership Information Sharing**

**1. Lesson Goals/Objectives:**

* Explain how information is shared within and across the critical infrastructure sectors under the NIPP.
* Describe the role of the SCCs and subordinate Information Sharing Working Groups in support of critical infrastructure and resilience information sharing.
* Describe the role of the DHS IP Partnership Programs and Information Sharing (PPIS) Branch in facilitating government-private partnership governance as well as Secretariat support for the GCCs and SCCs.
* Describe the role of CIPAC in enabling *cross sector* information sharing, protection, and coordination.
* Explain how the 24 x 7 NICC, NCCIC and the Homeland Security Information Network (HSIN) – Critical Sector (CS) system support the operation of the information sharing process within and among the critical infrastructure sectors.
* Describe the role of State and local EOCs in facilitating information sharing in the context of natural disasters and non-terrorist manmade threats and hazards.

**2. Discussion Topics:**

* What is the role of each SCC’s Information Sharing Working Group in establishing the process for each critical infrastructure sector?
* How are critical infrastructure sector recipients and/or HSIN-CS subscribers identified?
* Who develops and maintains each critical infrastructure sector’s distribution list?
* What are the roles of trusted intermediaries like Trade Associations and ISACs in extending the distribution lists?
* Who develops and maintains the Cross Sector critical infrastructure Leadership distribution list known as the Executive Notification Service (ENS) list?

How is the ENS used to convene an emergency conference call or Webinar when there has been a major terrorist threat\attack or the national threat level is about to change? Give an example as described in the NIPP.

* How do the critical infrastructure sectors and the NICC distinguish between routine and crisis information sharing and communications? How is that distinction reflected in their mode of interaction?
* How does CIPAC promote and support cross sector information sharing? Give examples.
* What arrangements have State and Local Fusion Centers made to share their sensitive and Law Enforcement Sensitive (LES) information with critical infrastructure sector entities within their jurisdiction? Do critical infrastructure sector entities have a physical or virtual presence in Fusion Centers? Should they?
* If Intelligence is obtained at the Federal level that there is a credible facility-specific, asset-specific, or system-specific threat, how is that Intelligence communicated to the critical infrastructure owners and operators?

**3. Required Reading:**

The White House. *National Strategy for Information Sharing*. 2007.

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

U.S. Department of Homeland Security. *NIPP 2013, Partnering for Critical Infrastructure Security and Resilience*. 2013, pp. 1-4, appendices A-B. <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.

ISAC Council. *The Role of ISACs in Private/Public Sector CIP*. 2009.

http://www.isaccouncil.org/images/ISAC\_Role\_in\_CIP.pdf.

U.S. Gov’t Accountability Office GAO-04-780, *Critical Infrastructure Protection: Improving Information Sharing With Infrastructure Sectors*,(2004), <http://www.gao.gov/new.items/d04780.pdf>.

U.S. Department of Homeland Security. *Charter of the Critical Infrastructure Partnership Advisory Council (CIPAC)*. 2010. <http://www.dhs.gov/xlibrary/assets/cipac/cipac_charter.pdf>.

U.S. Gov’t Accountability Office GAO-08-636T, *Homeland Security: Federal Efforts are Helping to Address Some Challenges Faced by State and Local Fusion Centers*, (2008), http://www.gao.gov/products/GAO-08-636T.

U.S. Gov’t Accountability Office GAO-10-972, *Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results*, (2010), <http://www.gao.gov/products/GAO-10-972>.

**Lesson 7 Topic: Derailed: A Case Study of the 2001 Howard Street Tunnel Fire**

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

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

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

**2. Discussion Topics**:

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

**3. Required Reading**:

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

**Lesson 8 Topic: Information Sharing Lifecycle**

**1. Lesson Goals/Objectives:**

* Explain the six phases of the information sharing lifecycle, as well as how they relate to one another:
  + Requirements;
  + Collection/Storage;
  + Analysis;
  + Production;
  + Dissemination;
  + Feedback and Update
* Explain how SCCs, the ISACs, and critical infrastructure owners and operators participate in the requirements, collection, dissemination, and feedback phases.
* Explain how standing information needs (SINs) are developed.
* Analyze the roles and responsibilities of DHS/ I&A in collecting and disseminating intelligence from the IC as well as from DHS Law Enforcement components, and how they interact with State and local Fusion Centers throughout the information sharing life cycle.
* Describe the roles and responsibilities performed by the DHS/NICC across the information sharing life cycle during steady-state operations and incidents.

**2. Discussion Topics:**

* Why is the information sharing lifecycle a cyclical versus linear process?
* What roles do SCCs and critical infrastructure sector members play in the requirements phases for both information and intelligence? Cite statutes or directives where the private sector is given a role in the intelligence requirements phase. Give examples of events in which SCCs and/or critical infrastructure sector members have implemented that role.
* What is the role of the SSA in the information sharing lifecycle?
* What roles do SCCs and critical infrastructure sector members have in the feedback phase for both information and intelligence? Give examples of events in which SCCs and/or critical infrastructure sector members have implemented that role.
* What contribution do you think DHS organic Law Enforcement components such as U.S.Immigration and Customs Enforcement (ICE), Border Patrol, Transportation Security Administration (TSA), and U.S. Coast Guard can make to the Intelligence collection efforts of the DHS/Intelligence and Analysis Directorate?
* What roles do critical infrastructure owners and operators have in the collection phase, particularly concerning the preparation and submittal of Suspicious Activity Reports (SARs)? Do you feel that SARs represent ‘dots’ that should be connected to other dots by the IC and Law Enforcement? How can SARs ultimately result in better critical infrastructure security and resilience?
* Regarding the dissemination phase, compare and contrast the centralized DHS headquarters model to the decentralized and distributed State and Local Fusion Center model. Do you feel that critical infrastructure owners and operators need both kinds of models, and if so, why?

**3. Required Reading:**

Riegner, S. *Information Model for the Federal Aviation Administration's Airway Facilities Organization*. The MITRE Corporation. 1994. (Request MITRE Reports WP94W0000001 AC146 Box 439).

U.S. Air Force. *Requirements Development and Processing*. 1999. <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA405037>.

U.S. Department of Homeland Security. *Secretary Napolitano Announces Rail Security Enhancements, Launches Expansion of ‘See Something, Say Something’ Campaign*.2010.

<http://www.dhs.gov/ynews/releases/pr_1278023105905.shtm>.

U.S. Department of Homeland Security, Office of Intelligence & Analysis. *Strategic Plan Fiscal Year 2011- Fiscal Year 2018*. 2011. <http://www.dhs.gov/xlibrary/assets/ia-fy2011-fy2018-strategic-plan.pdf>.

U.S. Department of Homeland Security. *Office of Intelligence and Analysis Mission*. <http://www.dhs.gov/xabout/structure/gc_1305220817809.shtm>.

**4. Case Study Reflection Papers Due**

Turn in your case study reflection paper at the beginning of class per the instructions at the beginning of the syllabus.

**Lesson 9 Topic: Information Sharing Products**

**1. Lesson Goals/Objectives:**

* Explain how HSIN supports the Critical Infrastructure ISE.
* Describe the basic functionality of the HSIN-CS platform, how it aligns with user-generated requirements, and the various forms of trusted access and user verification common to the HSIN-CS system.
* Discuss the protocols and techniques used to develop information sharing products and the variety of types of products posted on HSIN-CS, to include:

**Tactical Products**

* Daily Open Source Infrastructure Report
* Suspected Terrorist Threats (Joint Intelligence Bulletins)
* Physical Threats
* Cyber Threats and Vulnerabilities
* Terrorist Tactics and Techniques
* Spot Reports (Incidents)
* Natural Disaster Situation Reports (SITREPS)
* Natural Disaster CI Damage Forecasts

**Strategic Products**

* Sector-Specific Threat Assessments
* Sector-Specific Risk Assessments
* Homeland Security Assessments
* National Risk Estimates
* Analyze the information sharing strategies, programs, networks, systems, and processes used by other Federal departments such as DOJ that have applicability to the Critical Infrastructure ISE.

**2. Homework:**

Develop a critical infrastructure security and resilience information sharing product and its associated transmittal cover sheet. Choose one of the following elevated terrorist threat conditions for researching retrospectively. The product should be prepared as if the event has not yet happened. In other words, learners are permitted to do “Monday morning quarterbacking” in preparing the product.

|  |  |
| --- | --- |
| Event | Date(s) |
| Hurricane Andrew | August 17, 1992 |
| U.S. postal system anthrax attacks | October 2001 and beyond |
| London transportation system bombings | July 7 and 21, 2005 |
| Hurricane Katrina | August 29, 2005 |
| Aviation threat level increase to Orange (liquid explosives) | August 10, 2006 |
| Christmas Day Aviation bomb attempt | December 25, 2009 |
| FEDEX and UPS Aviation cargo bombs | October 29, 2010 |
| Joplin, Missouri Tornados | May 22, 2011 (late afternoon) |
| Japan Earthquake and Tsunami | March 11, 2011 |
| Hurricane Irene | August 28, 2011 |
| Hurricane Sandy | October 30, 2012 |

|  |  |
| --- | --- |
| Event | Date(s) |
| U.S. postal system anthrax attacks | October 2001 and beyond |
| London transportation system bombings | July 7, 21 2005 |
| Aviation threat level increase to Orange (liquid explosives) | August 10, 2006 |
| Christmas Day Aviation bomb attempt | December 25, 2009 |
| FEDEX and UPS Aviation cargo bombs | October 29, 2010 |

The product should warn of the threat at least 24 hours before the date given in the table above. The product should be as specific as possible about the nature of the threat without being unrealistically specific in terms of the precise time and location of the attack and tactics employed. The product should recommend protective strategies and measures for the affected critical infrastructure sectors to take and describe what the government is doing to protect affected critical infrastructure. Learners should research and draw upon any terrorist risk assessments for the affected sectors available in the public domain. A transmittal sheet (cover page) should accompany the product stating who in DHS originated the product (e.g., DHS/Intelligence & Analysis or DHS/Transportation Security Administration), which sectors it should go to, and the date and time it should be transmitted. The product should be labeled with a (simulated) handling caveat such as For Official Use Only (Simulated) or Law Enforcement Sensitive (Simulated). The product and transmittal sheet are due one week from the date of this lesson (taking any holidays into account).

**3. Discussion Topics:**

* Why is it necessary to vet subscribers before granting them access to the Homeland Security Information Network - Critical Sector?
* How are subscribers alerted that a new product has been posted to the HSIN-CS or to one of the sector-specific portals?
* Why is HSIN-CS not used by all sectors for information dissemination? What are the draw backs to HSIN-CS use?
* Do you feel that the range of tactical and strategic products listed above cover the critical infrastructure security and resilience needs of most critical infrastructure owners and operators? If so, why? If not, why not?

**4. Required Reading:**

Federal Bureau of Investigation. *InfraGard Program*. <http://www.infragard.net/>.

Department of Justice. *Global Justice Information Sharing Initiative*. <http://www.it.ojp.gov/global>.

Haimes, Yacov Y. “Risk of Terrorism to Cyber-Physical and Organizational-Societal Infrastructures,” *Public Works Management & Policy* 6(4) (2002): 231-40. <http://pwm.sagepub.com/content/6/4/231.full.pdf+html>.

**Lesson 10 Topic: Sharing of Sensitive and Classified Information**

**1. Lesson Goals/Objectives:**

* Explain the various levels of classified and sensitive information.
* Describe the difference in legal status and penalties associated with unauthorized disclosure of classified and sensitive information.
* Assess the private sector’s role in maintaining sensitive and/or classified information.
* Explain how SBU and classified information can create barriers to sharing and discuss how these barriers can be overcome.

**2. Discussion Topics:**

* What are some of the authorized methods for sharing classified threat information with Sector Coordinating Council members?
* How can classified threat information be shared quickly with critical infrastructure owners and operators in the field who possess clearances?
* Is there a clear process within the intelligence community to prepare “tear lines” that can be shared with the general critical infrastructure community? Do these tear lines still contain useful or actionable information that will benefit the critical infrastructure community?
* What can a cleared private sector partner actually do with classified information? How can classified threat information that is shared with the Chief Security Officer at a company’s headquarters be used to protect infrastructure in the field?
* What role can State and local Fusion Centers play in sharing classified information with CI owners and operators in their jurisdiction?
* Does DHS have authority and procedures to certify critical infrastructure facilities (e.g., a national Trade Association) for the receipt, storage, review, discussion, and destruction of classified information?
* Why is “need-to-know” a necessary condition in addition to having the appropriate clearance for receipt of classified information?
* What is the expected outcome of the new Intelligence Community dictum “responsibility to share”? Do you believe it will achieve its expected outcome?
* Did the WikiLeaks event during December 2010 cause a ‘chill’ in information sharing (a shift back from “responsibility to share” to “need-to-know”)? What new guidance or security controls were issued as a result?
* If you were the President of the United States or a high ranking member of Congress what proposal would you make to streamline and improve the timeliness of classified information sharing with critical infrastructure owners and operators in the field?
* Do you think it is accurate to characterize critical infrastructure owners and operators in the field as front line defenders of our nation’s critical infrastructure and therefore justified in receiving classified intelligence information?
* How will the new designation of Controlled Unclassified Information as applied to various types of sensitive but unclassified enhance the ability to share that sensitive but unclassified information?

**3. Required Reading:**

Exec. Order No. 12,958. *Classified National Security Information, as Amended*. 2003. <http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html>.

### Exec. Order No. 13,292. Further Amendment to Executive Order 12,958, as Amended,

### Classified National Security Information. 2003. <http://www.fas.org/sgp/bush/eoamend.html>.

# Exec. Order No. 13,526. *Classified National Security Information*. 2009.

<http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information>.

Exec. Order No. 13,556. *Controlled Unclassified Information*. 2010. <http://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-controlled-unclassified-information>.

Warrick, J. “[WikiLeaks Cable Dump Reveals Flaws of State Department's Information-Sharing Tool](http://www.washingtonpost.com/wp-dyn/content/article/2010/12/30/AR2010123004962.html?referrer=emailarticle).”*Washington Post*, December 30, 2010. Assessed June 23, 2014<http://www.washingtonpost.com/wp-dyn/content/article/2010/12/30/AR2010123004962.html?wprss=rss_technology>.

**Lesson 11 Topic: Systems & Tools for Sharing Sensitive and Classified Information**

**1. Lesson Goals/Objectives:**

* Evaluate the systems commonly used for sharing SBU\CUI with critical infrastructure owners and operators and State and local homeland security officials, including the following:
  + HSIN-CS
  + US-Computer Emergency Readiness Team (US-CERT) for critical infrastructure owners and operators
  + HSIN –Intel/Homeland Security State and Local Intelligence Community of Interest (HS-SLIC) for State and local homeland security officials
* Identify the two commonly used classified information sharing systems:
* Homeland Secure Data Network (HSDN)
* Homeland Top Secret Network (HTSN) (interoperable with JWICS)
* Explain the steps for private sector partners and DHS contractors to gain and maintain authorized access to any DHS system that stores and transmits SBU or classified information:
* Having a DHS sponsor
* Vetting by the critical infrastructure sector or by DHS as a contractor or partner
* Having the appropriate clearance level and need-to-know
* Having been granted DHS Suitability
* Obtaining a user account on the system
* Passing the annual information security awareness test for the system
* Assess the specific training requirements for accessing CUI/SBU information and the rules and procedures for uploading and downloading information from/to electronic media (e.g., USB drives) from government systems.

**2. Discussion Topics:**

* Why are there strict rules about uploading any information onto a sensitive or classified system?
* What is a Sensitive Compartmentalized Information Facility (SCIF)? What use are SCIFs in a homeland Security context?
* What procedures would you expect to be in place for downloading For Official Use Only from a SECRET level system to a sensitive but unclassified system, or similarly, for downloading SECRET information from a TS system to a SECRET system?
* Do you think it’s possible to securely electronically connect systems at different classification levels or should they be air-gapped? What are the tradeoffs?
* How can an enterprise digital rights management system (eDRM) be used to control who can access certain sensitive but unclassified information and what they are permitted to do with it? How can enterprise digital rights management system be used to enhance information sharing?

**3. Required Reading:**

U.S. Department of Homeland Security, Office of the Inspector General. *DHS’ Efforts to Improve the Homeland Security Information Network*.2008.

<http://www.oig.dhs.gov/assets/Mgmt/OIG_09-07_Oct08.pdf>.

U.S. Department of Homeland Security, *About the Homeland Security Information Network*, (2010), <http://www.dhs.gov/files/programs/gc_1156888108137.shtm>.

U.S. Department of Homeland Security. *Homeland Security State & Local Intelligence Community of Interest (HS SLIC).* 2010. <http://www.dhs.gov/files/programs/gc_1233582654947.shtm>.

U.S. Government Accountability Office GAO-09-40, *Information Technology: Management*

*Improvements Needed on the Department of Homeland Security’s Next Generation Information Sharing System*, (2008), <http://www.gao.gov/new.items/d0940.pdf>.

U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team. *Welcome to US-CERT*. 2010. <http://www.us-cert.gov/>.

**Lesson 12 Topic: Standard Operating Procedures (SOPs) for Maintaining Critical Infrastructure Information Sharing Portals**

**1. Lesson Goals/Objectives:**

* Explain and evaluate the basic building blocks that comprise an effective Standard Operating Procedure (SOP) for a Critical Infrastructure Information Sharing Portal or Network such as HISN-CS or others as adopted by the critical infrastructure sectors:
* Nominating, Vetting, and Validation
* Data Management Process
* Routine Communication
* Incident Communication
* Alerts, Warnings, and Notifications
* Suspicious Activity Reporting
* Assess how the various sectors tailor the basic building blocks above to meet sector needs.

**2. Discussion Topics:**

* Does the Nominating, Vetting, and Validation Standard Operating Procedure limit the Portal access to just private sector members of the sector or are Federal, State, and local government sector able to join?
* Is the Data Management Process fully the responsibility of the Sector Coordinating Councils Information Sharing Working Group or can DHS/IP provide some support (e.g., with refreshing information)?
* Does the Data Management Process Standard Operating Procedure specify what data is permissible to post and what is not? If inappropriate data were posted, what recourse would the Information Sharing Working Group have?
* Do any of the Standard Operating Procedures cross reference information management tools that are made available by the National Infrastructure Coordination Center off of links on the Homeland Security Information Network - Critical Sector homepage, e.g., the Integrated Common Analytical Viewer (iCAV) Geographic Information System?
* Using the Food and Agriculture (F&A) Routine Communication SOP as an example, what type of data will be routinely posted to the Food and Agriculture Portal?
* Using the Food and Agriculture Incident Communication SOP as an example, what type of data will be posted during incidents (e.g., terrorist attacks, natural disasters) to the Food and Agriculture Portal?
* Are sectors permitted to post their own Alerts, Warnings, and Notifications independent of what the National Infrastructure Coordination Center posts to the Homeland Security Information Network - Critical Sector homepage?
* Are sectors permitted to change the color-coded threat levels for their sector independent of what DHS does with the National Terrorism Advisory System (NTAS)? [at [www.dhs.gov/files/programs/ntas.shtm](http://www.dhs.gov/files/programs/ntas.shtm) ] See, for example, the Electric Sector Information Sharing and Analysis Center Portal at [www.nerc.com/page.php?cid=6|69|312](http://www.nerc.com/page.php?cid=6|69|312).
* Do you think that most sectors would be interested in developing a voluntary SARs SOP? What about those sectors that have mandatory SARs requirements from a regulatory agency? Can you see any value to having both types of SARs systems?
* In what way do you think that fusing SARs information with national Intelligence would help the Government in “connecting the dots”?

1. **Required Reading:**

Department of Homeland Security. *National Terrorism Advisory System (NTAS)*. [www.dhs.gov/files/programs/ntas.shtm](http://www.dhs.gov/files/programs/ntas.shtm).

Department of Justice. *Nationwide SAR Initiative (NSI)*. 2010. <http://nsi.ncirc.gov>.

**Lesson 13 Topic: Other Information Sharing Mechanisms**

**1. Lesson Goals/Objectives:**

* Evaluate the variety of additional information sharing mechanisms used to support the NIPP government-private partnership and enable information sharing between key critical infrastructure and resilience partners, including:
* DHS email
* Smart phones/Personal Digital Assistants
* Teleconferences
* Webinars
* Digital Billboards
* Chat on HSIN-CS
* Video Teleconferences (VTCs)
* DHS Blogs (<http://blog.dhs.gov> )
* DHS PSAs
* Law Enforcement Online (LEO)
* Regional Information Sharing System
* InfraGard
* Conferences, Summits, and Workshops
* Assess the potential for emerging technologies to promote collaborative information sharing.
* Explain how social networking media can be used to promote critical infrastructure information sharing within and across sectors and by various levels of government.

**2. Discussion Topics:**

* Which one of the other information sharing mechanisms do you feel is the best means of sharing information? You may want parse your answer into routine vs. incident information sharing.
* When Secure Mobile Environment – Portable Electronic Devices become available (e.g., as government furnished COMSEC equipment) for critical infrastructure owners and operators use, what do you see as their advantages for sharing classified information?
* Since Secure Mobile Environment – Portable Electronic Devices will be Government controlled COMSEC items, and only available in limited quantities, who should get them in the critical infrastructure sectors? What criteria should the Government use in allocating these scarce items?
* What are the advantages for communicating during a national crisis of having subscribed to the GETS and WPS services?
* What would be the risks of using social networking media to communicate about a terrorist threat to, or attack on, the Homeland? Does your analysis change if the threat is a natural disaster?
* What would be some innovative ways for Emergency Management or First Responders to use social networking media to communicate during a natural disaster?
* What are some of the drawbacks associated with the use of mobile devices in this arena?
* What are some other solutions to the issues presented by the various mechanisms and technologies by which information is shared?

**3. Required Reading:**

U.S. Department of Homeland Security. “The Blog @ Homeland Security,” (2014), <https://www.dhs.gov/news-releases/blog>.

# U.S. Department of Homeland Security, *Protective Security Advisors*.

<http://www.dhs.gov/files/programs/gc_1265310793722.shtm>.

# U.S. Department of Homeland Security, *Protective Security Advisors*.

<http://www.dhs.gov/files/programs/gc_1265310793722.shtm>.

**Secure Products Wiki. *General Dynamics Sectera Edge Secure Mobile Environment Portable Electronic Device (SME PED)*. 2010.** <http://www.secureproductswiki.com/SCIPProducts/GDSecteraEdge>.

L-3 Guardian®.***Secure Mobile Environment Portable Electronic Device (****SME PED)*. 2010.

<http://www2.l-3com.com/cs-east/pdf/l-3%20guardian%20faqs.pdf>.

Federal Bureau of Investigation. *LEO*. <http://www.fbi.gov/about-us/cjis/leo>.

Federal Communications Commission. *Government Emergency Telecommunications Service*.

2010. <http://transition.fcc.gov/pshs/services/priority-services/wps.html>.

National Communications System, “Government Emergency Telecommunications Service,” (2010), <http://transition.fcc.gov/pshs/services/priority-services/gets.html>.

Regional Information Sharing Systems. *RISS*. <http://www.riss.net/>.

**4. Additional Recommended Reading:**

Comfort, Louise K. "Risk and Resilience: Inter-Organizational Learning Following the Northridge Earthquake of 17 January 1994." *Journal of Contingencies and Crisis Management* 2(3) (1994): 157-70. <http://www.cdm.pitt.edu/Portals/2/PDF/Publications/RISK_AND_RESILIENCE.pdf>.

# U.S. Department of Homeland Security. *2011 Chemical Sector Security Summit*. 2011.

http://www.dhs.gov/xlibrary/assets/2011-chemical-security-summit-carafano.pdf.

Dinh, T.L. and Nguyen-Ngoc, A.V. “A Conceptual Framework for Designing Service Oriented Inter-Organizational Information Systems.” *Proceedings of the 2010 Symposium on Information and Communication Technology* (2010): 147-154.

<http://dl.acm.org/citation.cfm?id=1852640&bnc=1>.

Longstaff, P.H. "Security, Resilience, and Communication in Unpredictable Environments Such as Terrorism, Natural Disasters, and Complex Technology," Edited by Center for Information Policy Research. Cambridge, MA: Harvard University, 2005. <http://pirp.harvard.edu/pubs_pdf/longsta/longsta-p05-3.pdf>.

**Lesson 14 Topic: Delivery and Presentation of Research Papers**

**1. Lesson Goals/Objectives:**

* Deliver the course research paper to the instructor in accordance with the due date (i.e., by the last class)
* Demonstrate the ability to succinctly summarize and present the research paper in 10 – 20 minutes (depending on class size)
* Have the opportunity for an open and wide-ranging discussion of any of the information sharing topics or issues covered during the course

**2. Discussion Topics:**

* There are no pre-identified discussion topics since class time will be used for research paper presentations and for open discussion.

**3. Required Reading:**

* There are no required readings.

**Lesson 15 Topic: Delivery and Presentation of Research papers**

**1. Lesson Goals/Objectives:**

* Deliver the course research paper to the instructor in accordance with the due date (i.e., by the last class)
* Demonstrate the ability to succinctly summarize and present the research paper in 10 – 20 minutes (depending on class size)
* Have the opportunity for an open and wide-ranging discussion of any of the information sharing topics or issues covered during the course

**2. Discussion Topics:**

* There are no pre-identified discussion topics since class time will be used for research paper presentations and for open discussion.

**3. Required Reading:**

* There are no required readings.