**Certificate Program in Critical Infrastructure Security and Resilience**

**Course Number: XXXX**

**Course: Partnering and 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-level course provides an overview of partnerships and information sharing within the homeland security enterprise with a focus on the collaboration and information products, processes, and systems necessary to protect and enhance the resilience of the Nation’s critical infrastructure. The sharing of information among key government and private-sector stakeholders, during both steady-state operations and in response to emergent threats and incidents, is vitally important to the critical infrastructure mission area. In fact, information sharing provides a critical foundation for this mission area across the spectrum of prevention, protection, mitigation, response, and recovery.

This is a multi-faceted course that will expose learners to complex government-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 government and private sectors. It also includes a practical examination of partner roles and responsibilities and interaction through an interactive tabletop (or, alternatively, computer lab) exercise, the development and dissemination of a threat-warning product, research paper, and oral presentation. The overall goal is for learners to gain insights into how the proper fusion and sharing of information can lead to timely and actionable products that, in turn, will enable government and private sector owners and operators at all levels to accomplish their responsibilities under the National Infrastructure Protection Plan (NIPP). Finally, the course will demonstrate how information sharing can serve as an enabler to foster a partnership-focused and networked protection, resilience, and incident management regime.

**credits conferred:** 3

**prerequisites:** Foundations of Critical Infrastructure Security and Resilience

**learner outcomes/objectives (as mapped against the u.s. department of homeland security (dhs) critical infrastructure core competencies):**

This course is designed to enable learners to:

**1. Explain the authorities, roles, responsibilities, and capacities of key government and private sector critical infrastructure stakeholders regarding “all-hazards” homeland security information sharing:**

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

**2. Identify and assess “all-hazards” critical infrastructure partnership frameworks, information sharing processes and systems, and coordination/collaboration challenges:**

* Federal, State, local, tribal, territorial, regional, and private sector
* International collaboration, coordination, and communication
* Critical infrastructure data collection, warehousing, and protection
* Connecting the “Four Ps:” People, Processes, Products, and “Pipes”
* Systems challenges and opportunities

**3. Evaluate the critical infrastructure** p**artnership in action: national critical infrastructure information sharing foundations, frameworks, selected sector procedures, case studies, and in-class exercise:**

* National Terrorism Advisory System (formerly Homeland Security Advisory System) Alerts (e.g., Aviation Subsector)
* Anthrax attacks through the U.S. postal system (2001)
* Northeast Power Blackout (2003)
* Madrid and London Transit Bombings (2004/2005)
* Hurricane Katrina (2005)
* I-35W Mississippi River Bridge Collapse (2007)
* Christmas Day Bomb Threat (2009)
* Aviation Cargo Parcel Bombs (2010)
* Hurricane Sandy (2012)
* Boston Marathon Bombing (2013)
* Terrorist Surveillance of a Nuclear Power Plant (notional-exercise)
* Various Natural Disasters and Unintentional Manmade Events

**delivery method/course requirements:**

Course delivery will be through directed readings, class participation, information sharing product preparation, research paper, information sharing exercise, and in-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.

The assigned course readings 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 (GAO), Congressional Research Service (CRS), 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, particularly the external reviews, and from multiple perspectives. The instructor will facilitate the discussion by asking different levels of questioning (factual, analytical, and application of the material) to evaluate the depth of the learner’s comprehension of the content.

**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 notify your instructor in a timely fashion.
3. The completion of all readings assigned for the course is assumed. Since class will be structured around interactive 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%

Information Sharing Exercise 25%

Research Paper 35%

Research Paper Presentation 5%

**activities, exercise, and research projects:**

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

Each learner will develop a 3-4 page threat-warning information sharing product detailing threat information and recommended protective measures based on an actual historical incident. Details are provided in the Lesson 8 description below.

1. **Research Paper/Oral Presentation: (40%)**

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 will be structured/graded according to the following organizational format: problem statement, background (include key players, authorities, resources, etc.), discussion (presentation of alternatives with the identification of pros and cons for each alternative), and recommendations (including rationale behind their selection). Footnotes and citations 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.

Examples of research paper topic areas include (but are not limited to) the following:

* Lack of nationwide awareness of the existence of the government-private partnership for critical infrastructure, and how to participate in it, including its supporting information sharing mechanisms.
* Lack of a national integrated communications-collaboration-information system that operates at all required classification levels.
* Complexities associated with obtaining and maintaining security clearances for key elements of the private sector.
* 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, including staffing, subject-matter experts, and compensation for time and travel.
* Inadequate attention paid to the front end of the information sharing lifecycle, namely the defining of critical infrastructure information and intelligence needs and requirements.
* Lack of 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.
* Fear 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.
* The challenges involved with sharing information among and between different agencies, including resistance to sharing information.

Each learner will present a **summary** of his/her research topic (no more than 20 minutes in length) to the class during Lessons 14-15. The presentation format will mirror that of the research paper outline. **Research papers will be submitted either in person or electronically by the beginning of class on Lesson 15.** 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 Exercise: (25%)**

Learners will participate in a role-based, interactive tabletop, or computer lab information sharing exercise simulating a terrorist threat to multiple critical infrastructure sectors. In preparation for the exercise, each learner will develop a short 2-3 page paper in talking point format delineating his/her assigned role-based responsibilities during the exercise play. **This paper will be submitted at the beginning of class on the day of the classroom exercise (Lesson 13).** Additional details are provided in the Lesson 13 description below.

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

Participation includes coming to class prepared, participating in class discussion, and realistic role playing during the critical infrastructure information sharing exercise. Percentage points earned will be based upon proactive participation in the aforementioned activities.

**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 interim in-class evaluations at the end of Lesson 6, following conclusion of the information sharing exercise in Lesson 13, 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 course research paper, oral presentation, and information sharing product paper. Ongoing dialogue with the instructor regarding research paper development, oral presentation preparation, and incident management exercise preparation is highly encouraged.

**course textbooks:**

The following textbook is identified as the primary textbook for the course. This textbook will be supplemented by additional readings for each lesson, accessible on-line (with website addresses provided in the lesson description sections) or provided by the instructor. **An additional compendium of supplemental readings is provided in Attachment 1.**

Bullock, Jane, Haddow, George, Coppola, Damon P,. and Yeletaysi, Sarp. *Introduction to Homeland Security, Fourth Edition: Principles of All-Hazards Response*, Burlington, MA: Butterworth-Heinemann, (2012). <http://www.amazon.com/Introduction-Homeland-Security-Fourth-Edition/dp/0124158021>.

**grading scale (suggested--school policy dependent):**

**course outline**

**lesson 1 topic: the need for partnership and 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.
* Describe the evolution of critical infrastructure security and resilience partnerships and information sharing (and related lexicon) as a national policy focus area.
* Compare and contrast information sharing needs 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.
* Assess information sharing needs among various stakeholders prior to, during, and after an incident.
* Evaluate the need for routine information sharing to support government-private sector planning and resource investment for critical infrastructure security and resilience.

**2. Discussion Topics:**

* What were the barriers to information sharing and partnerships between elements of the IC and the Law Enforcement community (e.g., Federal Bureau of Investigation (FBI)) prior to September 11, 2001? Between government and the private sector at all levels prior to September 11, 2001?
* Which barriers were legislative/regulatory in nature and which were institutional/cultural prior to September 11, 2001? How have these barriers been reduced over time? What are the major impediments that remain?
* What did the President’s Commission on Critical Infrastructure Protection (1996-98) recommend regarding government-private partnerships and information sharing? Which recommendations were implemented prior to the September 11, 2001 attacks?
* How were government-private partnerships and information sharing addressed in U.S. government policy and strategy after the September 11, 2001 attacks and the decade that followed?
* How would you characterize the differences — with respect to ease, speed, and content — associated with 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?
* How did the WikiLeaks event during December 2010 illustrate that making information sharing too easy without proper controls can lead to misuse and leaking of sensitive and classified information?
* Give an example, real or hypothesized, of how government and industry might share risk information for purposes of conducting critical infrastructure security and resilience planning and resource investment.
* Give an example of an incident in which, for various reasons, agencies did and did not share information.

1. **Required Reading:**

Textbook: Chapters 1-2.

Marsh, Robert T.*, Critical Foundations: Protecting America’s Infrastructures*.1997. <http://www.fas.org/sgp/library/pccip.pdf>.

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

U.S. Department of Homeland Security. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*.2003.<http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.

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

Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, (2013), <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

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

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

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>.

**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>.

Office of the Director of National Intelligence. *United States Intelligence Community Information Sharing Strategy*2008. <http://www.fas.org/irp/dni/iss.pdf>.

*Ten Years After 9/11: A Status Report on Information Sharing: Hearing by the Senate Comm. on Homeland Security and Governmental Affairs*, (2011). <http://www.hsgac.senate.gov/hearings/ten-years-after-9/11-a-status-report-on-information-sharing>.

U.S. Department of Homeland Security. *Homeland Security: Protecting, Analyzing, and Sharing Information*. 2008. <http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf>.

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>.

**lesson 2 topic: legislative and executive policy mandates for information sharing**

**1. Lesson Goals/Objectives:**

* Identify the various acts of legislation and Executive Orders and policies governing government-private sector partnerships and information sharing.
* Discuss the concepts and functions associated with the Information Sharing Environment (ISE), including the ISE private sector component.
* Evaluate how the government and private sector collaboratively share information in an all threats, all hazards environment.

1. **Discussion Topics:**

* Why was there a need to enact the Intelligence Reform and Terrorism Reduction Act subsequent to Homeland Security Act of 2002? What new authorities were provided and to whom did they apply? Is this system working?
* 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 these legislative or executive mandates direct or request the private sector to share information?
* How does the Federal government, particularly DHS and FBI, share threat information with the critical infrastructure sectors?
* What is the Protected Critical Infrastructure Information Program (PCIIP)? Is it effective?
* How does the NIPP address all-hazards information sharing and critical infrastructure partnerships between various levels of government and the private sector?
* 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 does the Quadrennial Homeland Security 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? What issues remain to be resolved?

1. **Required Reading:**

Textbook: Chapters 3-4.

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

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

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. *Guidelines and Requirements in Support of the Information Sharing Environment*. (2005.

<http://www.fas.org/sgp/news/2005/12/wh121605-memo.html>.

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

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

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.

U.S. Department of Homeland Security Information Sharing Governance Board. *DHS Strategy for Information Sharing*. 2008. <http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf>.

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

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

Information Sharing Environment. ”Information Sharing and the Private Sector.” Accessed June 19, 2014.<http://ise.gov/sharing-private-sector>.

1. **Additional Recommended Reading:**

Information Sharing Environment. *Information Sharing Environment Implementation Plan.* 2006. <http://ise.gov/sites/default/files/ise-impplan-200611_0.pdf>.

Prieto, Daniel B. “Information Sharing with the Private Sector: History, Challenges, Innovation, and Prospects.” In [*Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*](http://belfercenter.ksg.harvard.edu/publication/1977/seeds_of_disaster_roots_of_response.html?breadcrumb=%2Fpublication%2F2516%2Fwhere_private_efficiency_meets_public_vulnerability), edited by in Lewis M. Branscomb,Philip E. Auerswald, Todd. M. La Porte, and Erwann O. Michel-Kerjan, chap. 23. Cambridge University Press, 2006. <http://www.policyarchive.org/handle/10207/bitstreams/5587.pdf>.

Auerswald, Philip E., Branscomb, Lewis M., La Porte, Todd M., and Michel-Kerjan, Erwann O. “Where Private Efficiency Meets Public Vulnerability: he Critical Infrastructure Challenge.” In [*Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*](http://belfercenter.ksg.harvard.edu/publication/1977/seeds_of_disaster_roots_of_response.html?breadcrumb=%2Fpublication%2F2516%2Fwhere_private_efficiency_meets_public_vulnerability), edited by Lewis M. Branscomb,Philip E. Auerswald, Todd. M. La Porte, and Erwann O. Michel-Kerjan, chap. 1. Cambridge University Press, 2006. <http://opim.wharton.upenn.edu/risk/seedsofdisaster/Chapter_1.pdf>.

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

Information Sharing Environment. *Annual Report to the Congress.* 2010.

<http://www.nctc.gov/itacg/docs/ISE-Annual-Report-to-Congress-2011.pdf>.

Information Sharing Environment. *Annual Report to the Congress.* 2011. <http://ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2011.pdf>.

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

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

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

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

**lesson 3 topic: establishing the foundation for successful information sharing**

**1. Lesson Goals/Objectives:**

* Describe and 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 senior leadership/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? How do we define the “value proposition” for public-private information sharing?
* What are some of the most effective communication and workflow processes and practices associated with multi-level information sharing?
* What kinds of specialized skills, training, and education do government and the private sector need in order to sustain a successful information sharing community?

**3. Required Reading:**

Textbook: Chapters 5-6.

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

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.

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

Perseus Books: Cambridge, 1996. U.S. Department of Homeland Security. “Counterterrorism Publications: Protecting, Analyzing & Sharing Information.” Accessed June 19, 2014. <http://www.dhs.gov/counterterrorism-publications>.

Information Sharing Environment. ”Information Sharing and the Private Sector.” Accessed June 19, 2014.<http://ise.gov/sharing-private-sector>.

**lesson 4 topic: building a framework for multi-dimensional information sharing**

**1. Lesson Goals/Objectives:**

* Identify and evaluate the five-dimensional framework for effective information sharing.
* 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.

**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 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?
* Within the government-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 the principal types and sources of information that support the critical infrastructure security and resilience mission?
* How can implementing performance metrics and feedback mechanisms enhance information sharing? What are some key examples?

1. **Required Reading:**

Textbook: Chapters 7-8.

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>.

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>.

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>.

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>.

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>.

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>.

**lesson 5 topic: information sharing partnerships and processes**

**\*\* special activity: research paper topic submissions due via e-mail by the beginning of class.**

**1. Lesson Goals/Objectives:**

* Identify 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)
* Identify the key organizations that have formed to facilitate critical infrastructure security and resilience information sharing
* Evaluate the contributions of State, local, and regional Fusion Centers in the context of the critical infrastructure security and resilience mission area:
* Information gathering requirements
* Intelligence analysis and production capabilities
* Information/intelligence sharing and dissemination
* Prevention, protection, mitigation, response, and recovery
* 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 — daily and in the context of emerging threats and incidents?
* What role does each of the following organizations play in critical infrastructure security and resilience information sharing?
* SCCs
* SSAs and GCCs
* SLTT-GCC
* Regional Consortia
* CIPAC
* ISACs and the ISAC Council
* State and local Fusion Centers
* JTTFs
* EOCs
* DHS/ I&A
* DHS/ NICC
* DHS/ PSAs and Regional Mission Collaboration Staff
* DHS/ FEMA
* How is information shared between the entities identified above in the context of terrorist threat information? Information regarding other hazards?
* How effective is the NIPP Partnership Model in achieving the necessary level and quality of information sharing required to execute the critical infrastructure security and resilience mission?
* What special coordination role does the SSA play in information sharing?
* 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?
* What type of critical infrastructure security and resilience capacities are recommended in the joint DOJ-DHS Fusion Center baseline guidance?
* What information does the government need from the private sector in order to build its risk management budgets, plans, and policies?
* How effective have the Fusion Centers been regarding developing critical infrastructure security capabilities, including information sharing with local critical infrastructure owners and operators?

**3. Required Reading:**

Textbook: Chapters 9-10.

*A Functional Model for Critical Infrastructure Information Sharing and Analysis*, (2004),

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

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

Department of Homeland Security, *State and Local Fusion Centers*, (September 2009),

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

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>.

U.S. Department of Homeland Security, *Fusion Centers and Joint Terrorism Task Forces*, <http://www.dhs.gov/files/programs/gc_1298911926746.shtm>.

Federal Bureau of Investigation, *Terrorism*, <http://www.fbi.gov/about-us/investigate/terrorism/terrorism>.

# Additional Recommended Reading:

# 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>.

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>.

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

U.S. Department of Homeland Security, Emergency Management Institute. *IS-650.a Building Partnerships with Tribal Governments*. <http://training.fema.gov/EMIWeb/IS/is650a.asp>.

ISAC Council. *National Council of ISACs*. <http://www.isaccouncil.net/>.

**lesson 6 topic: information sharing under the nipp partnership framework**

**1. Lesson Goals/Objectives:**

* Assess the information sharing process within and across the critical infrastructure sectors under the NIPP.

**2. Discussion Topics:**

* What is the role of each SCC’s Information Sharing Working Group in establishing information sharing processes and protocols for each critical infrastructure sector?
* How are critical infrastructure sector information recipients and/or Homeland Security Information Network (HSIN) – Critical Sector (CS) (HSIN-CS) subscribers identified?
* What is the role of NICC and NCCIC in facilitating steady-state and incident-related information sharing among NIPP partners?
* What are the roles of trusted intermediaries like Trade Associations and ISACs in critical infrastructure and resilience information sharing?
* How is the Executive Notification Service (ENS) used in the context of an emergent threat or natural disaster situation? Give an example as described in the 2014 NIPP.
* How do the critical infrastructure sectors and 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 critical infrastructure owners and operators?

**3. Required Reading:**

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>.

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

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

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. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013, pp. 10-12, Appendix A. <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.

Robert Riegle Testimony Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment, *The Future of Fusion Centers: Potential Promise and Dangers*, (2009), <http://www.dhs.gov/ynews/testimony/testimony_1238597287040.shtm>.

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-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: the information sharing lifecycle**

**1. Lesson Goals/Objectives:**

* Evaluate 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

**2. Discussion Topics:**

* Why is the information sharing lifecycle a cyclical versus linear process?
* What is the role of the DHS Office of Intelligence and Analysis in the sharing of information within the NIPP Partnership Framework? How does the DHS I&A Strategic Plan 2011-2018 address information sharing with State and local government and private sector partners? State and local Fusion Centers?
* What roles do SCCs, ISACs 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 Federal SSAs under the NIPP structure 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), U.S. Customs and Border Protection (CBP), Transportation Security Administration (TSA), and the U.S. Coast Guard can make to the intelligence collection efforts of the DHS/I&A? How do these contributions support the critical infrastructure security and resilience mission area?
* 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 more effective and efficient critical infrastructure security?
* How are standing information needs (SINs) developed?
* 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?
* Does information sharing differ within the NIPP Partnership Framework based on whether we are in steady state operations or managing an emergent threat or incident management?

**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>.

**lesson 8 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. Pre-Class Assignment:**

Develop a 3-4 page critical infrastructure security information sharing product and its associated transmittal cover sheet. Choose one of the following elevated alert periods 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 |
| Boston Marathon bombing | April 15, 2013 |

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 regarding 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/I&A or DHS/TSA), 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 prior to the beginning of class in Lesson 9.**

**3. Discussion Topics:**

* What is HSIN-CS and how is it used? How does it support multi-dimensional information sharing within the Critical Infrastructure ISE?
* Describe and provide examples of the various functional aspects of HSIN-CS.
* How are specific requirements used to support the build-out of the various HSIN-CS sector-specific portals generated and validated?
* Why is it necessary to vet subscribers before granting them access to HSIN-CS?
* How are subscribers alerted that a new product has been posted to the HSIN-CS or to one of the sector-specific portals?
* How does HSIN-CS support the National Terrorism Advisory System (NTAS)?
* Why is HSIN-CS not used by all sectors for information dissemination? What are the draw backs to HSIN-CS use? What are the alternatives to HSIN-CS?
* Do you feel that the range of tactical and strategic products provided through the HSIN-CS platform cover the critical infrastructure security and resilience needs of most critical infrastructure owners and operators? If so, why? If not, why not?
* What other information sharing systems, networks, and programs support the Critical Infrastructure ISE? How do these interface with HSIN-CS?
* What is the InfraGard program? How does it support the Critical Infrastructure ISE?

**4. Required Reading:**

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>.

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

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

**lesson 9 topic: enabling the sharing of sensitive and classified information**

**\*\*special activity: information sharing product due via email prior to the beginning of class.**

**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:**

* Why is so much of homeland security information classified or designated sensitive-but-unclassified (SBU)?
* What are the major characteristics of the following information protection regimes: FOUO, LES, CVI, PCII, SGI, and SSI?
* What are some of the authorized methods for sharing classified threat information with SCC members and the Critical Infrastructure ISE writ large?
* How can classified threat information be shared quickly with critical infrastructure owners and operators in the field who possess clearances?
* Is there a streamlined, transparent process within the IC community to prepare “tear lines” that can be shared with the general critical infrastructure security and resilience community? Do these tear lines still contain useful or actionable information that will benefit the Critical Infrastructure ISE?
* 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 Federal IC field offices and State and local Fusion Centers play in sharing classified and other sensitive information with critical infrastructure owners and operators in their jurisdiction?
* How is sensitive information voluntarily provided to DHS by the private sector protected?
* 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 IC dictum “responsibility to share?” Do you believe it will achieve its expected outcome?
* Did the December 2010 WikiLeaks event 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?
* Are additional statutory or other authorities needed to streamline and improve the timeliness of classified information sharing between government and 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 CUI as applied to various types of sensitive but unclassified information enhance the ability to share that 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. 13,526. *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 10 topic: systems and 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)? How are SCIFs used in a homeland security context?
* What procedures would you expect to be in place for downloading FOUO 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?
* Is it 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?
* Do the specific training requirements for accessing CUI/SBU information adequately familiarize the user with the safeguarding and dissemination requirements for the information?
* How do private sector partners and DHS contractors gain and maintain authorized access to any DHS system that stores and transmits SBU or classified information?
* How do the rules governing access to various categories of sensitive information differ depending on the specific category?
* What are the commonly used Commercial-Off-The-Shelf tools that can control access to information based on an individual’s identity, role, or sector and that can enforce the need-to-know rule?

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

**lesson 11 topic: standard operating procedures (sops) for maintaining critical infrastructure 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:**

* How do the nominating, vetting, and validation processes affect private sector as well as government members of the portal community of interest? Are Federal, State, local, tribal, and territorial government sector partners able to join?
* Is the Data Management Process fully the responsibility of the SCC Information Sharing Working Groups or can DHS/IP provide some support (e.g., with refreshing information)?
* Does the Data Management Process SOP 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 SOP cross reference information management tools that are made available by NICC off of links on the HSIN-CS 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 F&A 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 F&A Portal?
* Are sectors permitted to post their own Alerts, Warnings, and Notifications independent of what NICC posts to the HSIN-CS homepage?
* Are sectors permitted to change the threat level for their sector independent of what DHS does with NTAS? [[www.dhs.gov/files/programs/ntas.shtm](http://www.dhs.gov/files/programs/ntas.shtm)] See, for example, the Electric Sector ISAC 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 SAR 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 12 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 of the various information sharing mechanisms identified above do you feel provides the best means of sharing critical infrastructure information? What are the advantages and disadvantages of each? Give examples.
* How do these mechanisms interface with HSIN-CS?
* Can these mechanisms be integrated into an all-hazards information sharing enterprise architecture, or do they represent unconnected “stovepipes?”
* When SME-PEDs become available (e.g., as government furnished Communications Security (COMSEC) equipment) for critical infrastructure owners and operators use, what do you see as their advantages for sharing classified information?
* Since SME-PEDs will be government controlled COMSEC items, and only available in limited quantities, who should get them within 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 Nation? 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 critical infrastructure-related concerns 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:**

**Flynn, S. *The Edge of Disaster: Rebuilding A Resilient Nation*. Chap. 8. Random House: New York, 2007.**

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

**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>.

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

Federal Communications Commission. *Government Emergency Telecommunications Service*. 2010. <http://transition.fcc.gov/pshs/services/priority-services/wps.html>.

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

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

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

**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>.

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>.

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

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

Klein, Ken. “FEMA Communicates with the Public via Digital Billboards.” *The CIP Report* 10(6). <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_December2011__NaturalDisasters2.pdf#page=.16>.

**lesson 13 topic: information sharing exercise**

**\*\*special activity: information sharing exercise point papers due via email prior to class.**

**1. Lesson Goals/Objectives:**

* Evaluate the complexities of sharing information regarding a specific threat to critical infrastructure and how threat-related information is communicated within the NIPP Partnership Framework (Federal, State, local, tribal, and territorial and private sector) in an emergent threat situation scenario as well as an incident in progress.
* Deconstruct the SARS process and explain the products, systems, processes, and protocols that support critical infrastructure information sharing as a component of SARS reporting and incident management operations.

**2. Exercise Scenario:**

The scenario initially involves the detection of possible pre-operational terrorist surveillance at various critical infrastructure facilities around the country, together with corresponding SARS reporting through appropriate channels. The scenario progresses to a credible, specific threat against various critical infrastructure facilities on the East Coast and in the Midwest. The scenario concludes with a terrorist attack on a critical infrastructure facility and the initial stages of the response (Federal, State, local, tribal, territorial, and private sector).

For the exercise, learners will be assigned roles and responsibilities corresponding to the various information sharing nodes described in the NIPP and other national and sector-level strategies and plans. Learners will “role play” their assigned position during the course of the exercise. Specific positions include:

* Security managers at surveyed critical infrastructure facilities
* DHS/ NICC
* DHS/ Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)
* FBI JTTFs
* State Fusion Center
* Local Law Enforcement
* SCC Chairpersons and ISACs
* Sector Specialists

Learners should refer to the material discussed throughout the course to prepare for their role-based play in the exercise. Additional research on-line or otherwise may be required to support geographic-specific roles within the scenario.

**3. Exercise Play:**

The instructor will serve as the facilitator to guide the exercise play and elicit input from role-based players. The exercise may be conducted either as a tabletop exercise or as computer lab information sharing event in which each individual or “node” is assigned to a workstation with the capability to project each workstation's screen onto a large wall display (e.g., a plasma TV screen). The computer lab version may enable the use of DHS-provided information sharing tools and systems with advanced coordination with DHS to obtain necessary approvals and security certifications.

1. **Discussion Topics:**

* What are the key government and private sector information sharing/incident management nodes according to the NIPP and the NRF?
* What are the information sharing roles and responsibilities of the various NIPP partners vis-à-vis national threat reporting and incident management?
* How are information and intelligence shared between the various government and private sector nodes of the NIPP Partnership Framework in an emergent threat scenario? Does the process work? What systems and technologies are involved and how are they used?
* How do the FBI, DHS, and local law enforcement share information with one another and with the private sector and in what sequence? What are the barriers to information sharing between the NIPP partners in the context of the exercise scenario?
* How does the National SARS Initiative function in the context of the exercise scenario? Are there gaps regarding stakeholder interaction, products, processes, and systems?
* What actions do the sectors take in response to a credible, specific threat? A national level NTAS elevation? How does this process work? How is information communicated within the sector? What is the role of the ISACs and other information sharing mechanisms?
* How is situational awareness maintained among the various NIPP partners during threat/incident response? What roles does the NICC play in this?

1. **Required Reading:**

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

U.S. Department of Homeland Security. *National Response Framework*. 2013. http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final\_national\_response\_framework\_20130501.pdf.

National Infrastructure Advisory Council. *Framework for Dealing with Disasters and Related Interdependencies*. 2009. <http://www.dhs.gov/xlibrary/assets/niac/niac_framework_dealing_with_disasters.pdf>.

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

U.S. Department of Homeland Security. *Fusion Centers and Joint Terrorism Task Forces*. <http://www.dhs.gov/files/programs/gc_1298911926746.shtm>.

Federal Bureau of Investigation. *Terrorism*. <http://www.fbi.gov/about-us/investigate/terrorism/terrorism>.

**lesson 14 topic: research paper presentations**

**1. Lesson Goals/Objectives:**

* Provide a concise summary of a key critical infrastructure security and resilience information sharing issue or a critical infrastructure security and resilience-related plan or policy and provide recommendations for improvement (Problem-Discussion-Recommended Solution format).

**2. Discussion Topics:**

* Presentations.

**3. Required Reading:**

* As required for research paper and presentation.

**lesson 15 topic: presentation of research papers and course critique**

**\*\*special activity: final research papers are due via e-mail prior to class.**

**1. Lesson Goals/Objectives:**

* Provide a concise summary of a key critical infrastructure security and resilience information sharing issue or a critical infrastructure security and resilience-related plan or policy and provide recommendations for improvement (Problem-Discussion-Recommended Solution format).
* Provide a forum for learner feedback on overall course content, method of instruction, and flow.

**2. Discussion Topics:**

* Presentations.
* Learner Course Evaluation: course content, flow, instructional methodology, etc.

**3. Required Reading:**

* As required for research paper and presentation.

**ATTACHMENT 1**

**CRITICAL INFRASTRUCTURE INCIDENT MANAGEMENT EXERCISE**

**TERRORISM SCENARIO**

**module 1: pre-incident suspicious activities (sar) reporting**

**1. Scenario Build**

* A well-known terrorist organization releases a new video to the international media trumpeting future attacks targeting European and American interests worldwide, with a particular emphasis on critical infrastructure facilities and systems within the energy, chemical, and critical manufacturing sectors. The video describes “striking at the heart of the corrupt and decadent Western economic system and the industries that support Western military power.”
* There is brief mention of the video in daily news reporting. The U.S. government provides a cursory official response to the video, but does not release any specific threat information related to the video.
* Extremist group Internet “chatter” and website activity are on the increase, with focused pronouncements of violent intent with near-term implications. The number of websites featuring home bomb-making instructions and terrorist operational surveillance techniques has proliferated greatly in recent months.

**2. Two Weeks Later**

* There is a marked increase in suspicious activity reporting from private sector sources in conjunction with numerous critical infrastructure facilities on the East Coast and in the Midwest. Examples include the following:
  + Two individuals operating from a white minivan were observed taking photographs at various sensitive locations outside the perimeter of the Calvert Cliffs Nuclear Power Plant in Southern Maryland. The individuals, the minivan, and the minivan license plate number were captured on video surveillance cameras operated by facility security personnel. Plant security officials initiated the SAR process in conjunction with the event and provided copies of the surveillance video to local law enforcement.
  + Outside the Cook Nuclear Power Plant in St. Joseph, Michigan, two individuals operating from a small recreational watercraft approximately one hundred yards offshore were observed taking pictures of the water approaches to the facility as well as various waterside security systems and barriers. The individuals and watercraft were captured on the facility security video surveillance system. Michigan Fish and Wildlife Law Enforcement Deputies responded to a call to investigate from plant security officials; however, the suspicious individuals had departed the area prior to their arrival. Local law enforcement is examining the facility surveillance videos for further information. Additionally, a SAR was initiated for this event.
  + Security officials at a major Dow Chemical production facility in Linden, New Jersey, reported that a Caucasian male in his early 30s attempted to enter the facility as a contract sanitation worker using false identification. Noticing the discrepancy in the documentation, the on-duty security official at the main visitors’ entrance stopped the individual and confiscated the ID badge. With this action, the suspect individual immediately ran to his car and fled the facility. The suspect, suspect’s vehicle, and out-of-state license plate number were captured on facility surveillance video. The video and confiscated ID badge were turned over to local law enforcement for review. A SAR was initiated for this incident.
  + Two suspicious individuals were observed by local utility operators on a routine inspection run taking photographs outside the western perimeter of a U.S. steel facility in Gary, Indiana. The utility operators immediately alerted U.S. steel security officials and provided a general description of the suspicious individuals and their vehicle. The individuals had departed the area by the time plant security personnel were able to respond. Two hours later, surveillance cameras at the Port of Indiana in the City of Portage captured two individuals on video matching the description of the men observed earlier by the utility workers in the vicinity of the U.S. steel plant taking pictures outside the facility perimeter. A SAR was initiated separately for each incident.

**3. Discussion Questions**

* What actions would the U.S. government be taking in response to the release of the terrorist video and website activity? The U.S. private sector? Do the contents and timing of release of this type of video and Jihadi website activity breech the “white noise” threshold?
* How does the SAR process work in the context of each of the individual events described above? Who are the major players involved? What actions does each take with respect to the specific information provided in the SAR?
* What systems are used to pass and protect SAR information and what products are generated?
* How do the initiators of the SAR receive feedback from the process?
* Are the SAR events described above distinguishable from day-to-day intelligence “white noise” from a U.S. government or private sector perspective?
* What is the role of the DHS/NICC in the SAR process? The local FBI JTTF? Local law enforcement? Local or regional fusion center?
* How would the information generated in each of the SAR events above be shared in a protected manner between private sector elements within the nuclear, chemical, and critical manufacturing sectors (ISACs, SCCs, associations, etc.)?
* How do the various agencies of the Federal government interact with Fusion Centers and other to “connect the dots” associated with the various individually reported SAR events discussed above?
* Would there be any changes recommended to protective measures across the critical infrastructure sectors of concern in the scenario based on the SAR events discussed above?

**module 2: emergent threat**

**1. Scenario Build**

* Officials in the United Kingdom (UK) apprehend an individual described as being an “operational chief” within the worldwide terrorist network. Although the individual’s identity is withheld from public disclosure, the UK government is collaborating closely behind the scenes with the U.S. IC regarding this individual. After initial questioning, the suspect provides general information regarding possible future attacks within Europe and the United States — focusing on energy infrastructure, high hazard chemical facilities, and internationally recognized manufacturing companies — and admits to casing targets associated with potential attacks against chemical and nuclear facilities in France and Germany during the previous year.
* Exact method, timing, and target location of these potential attacks are unknown, but, as the investigation proceeds, additional primary and secondary sources corroborate the suspect’s information. Questioning of additional sources indicate that a major attack within the United States may be in the final stages of operational planning.
* A new video is released on the Internet and on the Arab television station Al Jazeera from a terrorist affiliate responsible for previous attacks in Europe and Southwest Asia, boasting of pending suicide bomber attacks in the United States.
* In response to these developments, the FBI and DHS issue a joint intelligence bulletin warning of possible attacks against critical infrastructure facilities, systems, and personnel in the United States, with a special focus on the energy, chemical, and critical manufacturing sectors. Additionally, they conduct national conference calls and provide briefings on the specifics of the threat to critical infrastructure sector leadership.
* The U.S. government is *considering* increasing the national threat level to “Elevated” under the National Terrorism Advisory System (NTAS) with a focus on the above mentioned sectors. No definitive NTAS elevation decision has yet been made.

**2. Discussion Questions**

* What are your major personal and organizational concerns at this point?
* How would the process engage to ascertain whether or not any of the SAR reporting conducted during Module 1 is connected to this latest threat information?
* What would be the nature of any intelligence updates or products provided by the Federal government to the private sector and/or State and local government officials at this time? How would this process work?
* What are the systems used to enable this interaction, and how do they function in the context of this particular scenario?
* How are the NICC, NCTC, JTTFs, Fusion Centers and other key information sharing nodes engaging at this point, and with whom? How is the information being shared protected?
* How do U.S. critical infrastructure industries share terrorism-related threat information within sectors? Across sectors?
* What are the essential elements of intelligence and related information required by your jurisdiction, agency, community, industry, sector in the context of this scenario?
* How would the discussion related to the NTAS be framed? How does this process work? Is the private sector engaged in this process?
* What types of activities would the various key nodes of the NIPP incident management framework engage in at this point?

**module 3: initial incident response**

**1. Scenario Build (Present day)**

## 8:00 a.m. EDT

* Two large rental trucks laden with high explosives crash through the main gate at the Dow Chemical production facility in Linden, New Jersey, and detonate inside the facility. Although the explosions produce a large fireball on site, no critical assets or processes have been impacted, and there appears to be no off site chemical release. This incident occurred during the morning shift change, with maximum numbers of people on site. More than two dozen facility employees were killed or injured in the attack. All terrorist suspects were killed in the high explosive detonation.

## 8:10 a.m. EDT

* One large gasoline tanker truck crashes through the perimeter fencing at the Port of Indiana, in Portage, Indiana, and explodes just inside the facility gate, likely resulting from a premature detonation of an improvised explosive device. Half a dozen facility employees were killed or injured by the blast and ensuing fire. The port is closed to all landside and lakeside commercial activity. Local law enforcement and emergency responders are on scene.

* **8:15 a.m. EDT**
* A six-person suicide bomber squad shoots their way onto the premises of the Cook Nuclear Power Plant in St. Joseph, Michigan. En Route to the master control facility, they appear to be joined by two additional individuals wearing facility employee clothing who are provided weapons by the main assault team. Prior to reaching the control facility, the assault team is engaged and held in check by armed facility security guards operating from behind hardened defensive positions. Local sheriff’s deputies arrive on scene to help seal off the perimeter and reinforce the facility security guards. In the ensuing firefight, six terrorist suspects are killed and two are gravely wounded. They are immediately rushed to a local hospital in St. Joseph under heavy guard. Local FBI representatives are en route.

## 12:00 a.m. EDT

* An internet video is released from a heretofore unknown terrorist affiliate taking credit for the morning attacks and stating that there would be “more violent,” “near term” attacks to follow.

**2. Discussion Questions**

* What are your principal concerns and priorities in this phase of the scenario?
* What types of intelligence updates and information would be provided at this time, to whom, and by whom? How are the major information sharing nodes of the NIPP Partnership Framework interacting at this time?
* What are the systems used to enable this interaction, and how do they function in the context of this phase of the scenario? How is sensitive information protected through these systems?
* How are concerns regarding potential follow-on attacks addressed by government and the private sector? What types of information would be shared and by whom to mitigate the risk from a potential follow on attack(s)?
* How is information regarding terrorist tactics, techniques, and procedures collected, assessed, disseminated, and protected within the NIPP Partnership Framework, including facilities of a similar type to those attacked located in other areas of the country?
* How is situational awareness being maintained across government and between the government and the private sector during incident response?
* What key nodes of the National Response Framework and its Critical Infrastructure Support Annex are operational at this point? How do the law enforcement and emergency management communities share relevant information with one another at various levels in incidents like this?
* What information sharing activities are being undertaken by the sector operations centers, ISACs, SCCs, or other information sharing entities? The NICC?
* What are the key critical infrastructure sector dependencies/interdependencies that come to light as a result of this scenario? When and where do they first manifest themselves?
* How would you handle internal and external messaging of the events as they pertain to you and your organization, community, jurisdiction or sector? How is this messaging coordinated with external partners, including various levels of government and industry?