

**Course Number: XXXX**

**Course: Information Sharing for Critical Infrastructure Protection 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 Protection 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. Develop an understanding of the critical infrastructure Partnership in Action: National critical infrastructure information sharing foundations, frameworks, selected sector procedures, and in-class exercise:**

- 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
- Terrorist Surveillance of a Nuclear Power Plant (exercise)

**DELIVERY METHOD/COURSE REQUIREMENTS:**

Course delivery will be through readings as directed, 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 protection 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 beepers and cell phones should be turned off before class begins.

## **GRADING**

Class Participation	20%
Information Sharing Product	15%
Research Paper	35%
Research Paper Presentation	5%
Information Sharing Exercise	25%

## **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 8.

### **2. 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 should be completed using the following organizational format: problem statement, background (include key players, authorities, resources, etc.), discussion (presentation of alternatives with the identification of pros and cons for each alternative), and recommendations (including rationale behind their selection). Footnotes and citations, if any, should be included on a separate sheet of paper in the proper format for review. The paper should focus on the benefits, drawbacks, and obstacles to the practical application of proposed 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 Exercise (25%)**

Learners will participate in a role-based, interactive tabletop or computer lab information sharing exercise simulating a terrorist threat to a U.S. nuclear power plant. In preparation for the exercise, each learner will develop a short 2-3 page paper in talking point format delineating his/her assigned group role-based responsibilities during the exercise play. **This paper will be submitted at the beginning of class on the day of the classroom exercise.**

Details are given in Lesson 13.

#### **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 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 exercise, 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.

Jane Bullock, George Haddow, Damon P. Coppola, Sarp Yeletaysi, *Introduction to Homeland Security, Third Edition: Principles of All-Hazards Response*, Burlington, MA: Butterworth-Heinemann, (July 28, 2008).

#### **GRADING SCALE (SUGGESTED--SCHOOL POLICY DEPENDENT):**

## COURSE OUTLINE

### **LESSON 1 TOPIC: THE NEED FOR INFORMATION SHARING FOR CRITICAL INFRASTRUCTURE PROTECTION**

#### **1. Lesson Goals/Objectives:**

- Understand how the need for information sharing arose out of the Oklahoma City and 9/11 attacks
- Understand the differences in the needs for information sharing within the Intelligence Community (IC), between the IC, and other Federal agencies, DHS, and between DHS and Federal, State, tribal, territorial, local, and regional, private sector, and international partners
- Understand that Federal/State agencies and private sector companies must talk to each other; information that is not shared is information lost
- Understand the differences and similarities in the kinds of information that need to be shared before, during, and after a major natural disaster, a terrorist attack on the homeland, and other man-made events
- Understand the need for routine risk information sharing during public-private sector planning and budgeting for critical infrastructure protection and resilience
- Understand that as the Nation moves forward in securing its critical infrastructure, DHS must speak the language of business because unless the security measures bolster the bottom-line, they will not be implemented
- Understand that making sharing too easy without proper controls can lead to misuse and leaking of sensitive and classified information; the resulting backlash will then impede information sharing

#### **2. Discussion Topics:**

- What were the barriers to information sharing between elements of the IC and the Law Enforcement community (e.g., FBI) pre-911
- Which barriers were legislative/ regulatory and which were institutional/cultural pre-911?
- 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?
- How did the WikiLeaks event during December 2010 illustrate that making sharing too easy without proper controls can lead to misuse and leaking of 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 protection and resilience

### **3. Required Reading:**

Textbook: Chapters 1-2

*Implementing Recommendations of the 9/11 Commission Act of 2007*, (Public Law 110-53), August 3, 2007. <http://www.nctc.gov/docs/ir-of-the-9-11-comm-act-of-2007.pdf>.

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

*The 9/11 Commission Report*, July 22, 2004, Chapters 3, 8. <http://govinfo.library.unt.edu/911/report/index.htm>.

USA PATRIOT Act of 2001, <http://f11.findlaw.com/news.findlaw.com/wp/docs/terrorism/patriotact.pdf>.

### **4. Additional Recommended Reading:**

David Hoffman, *The Oklahoma City Bombing and the Politics of Terror*, 1998, [http://www.jrbooksonline.com/PDF\\_Books\\_added2009-4/ocbpt.pdf](http://www.jrbooksonline.com/PDF_Books_added2009-4/ocbpt.pdf).

U.S. House of Representatives, *The Need to Know: Information Sharing Lessons For Disaster Response*, Hearing before the Committee on Government Reform, March 30, 2006, <http://www.fas.org/sgp/congress/2006/infoshare.html>.

The White House, *The Federal Response to Hurricane Katrina - Lessons Learned*, February 23, 2006, <https://www.llis.dhs.gov/docdetails/details.do?contentID=15644>.

## **LESSON 2 TOPIC: LEGISLATIVE AND EXECUTIVE POLICY MANDATES FOR INFORMATION SHARING**

### **1. Lesson Goals/Objectives:**

- Understand that both Legislative and Executive branches of the government issued laws and policies, respectively, that directed information sharing (see Required Reading below)
- Understand why the 9/11 Commission report provided the foundation for much of the policy issuances that came afterwards  
Understand that the Homeland Security Act of 2002 assigned responsibility for threat information sharing to the Undersecretary for Information Analysis and Infrastructure Protection
- Understand that the Intelligence Reform and Terrorism Reduction Act of 2004 created the Information Sharing Environment (ISE) and it includes the Private Sector
- Learn that the *National Strategy for Homeland Security (2007)* and the *National Strategy for Information Sharing (2007)* promoted horizontal and vertical information sharing across the Federal, State, Local, tribal, territorial Governments and the Private Sector
- Learn that the Federal lead for the private sector portion of the Information Sharing Environment was assigned to DHS/Office of Infrastructure Protection
- Understand that Executive Order 12333, as amended in July 2008, reinforced the Intelligence Reform and Terrorism Reduction Act by giving the private sector a role in defining its intelligence and information requirements and in requiring the IC to disseminate the information that resulted from these requirements
- Understand that the *National Security Strategy of May 2010* requires all elements of the Federal Government to do everything in their power to prevent all threats and hazards from being realized and to enhance our resiliency in dealing with and recovering from those that occur

### **2. Discussion Topics:**

- Why was there a need to enact Intelligence Reform and Terrorism Reduction Act subsequent to 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?
- 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?  
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?

### **3. Required Reading:**

Textbook: Chapters 3-4

DHS, *Quadrennial Homeland Security Review Report*, February 2010, [http://www.dhs.gov/xabout/gc\\_1208534155450.shtm](http://www.dhs.gov/xabout/gc_1208534155450.shtm).

DHS, "Bottom-Up Review," July 2010, [http://www.dhs.gov/xabout/gc\\_1208534155450.shtm#1](http://www.dhs.gov/xabout/gc_1208534155450.shtm#1).

U.S. Government Accountability Office (GAO), *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GAO-08-492, June 2008, <http://www.gao.gov/new.items/d08492.pdf>.

Homeland Security Act of 2002, [http://www.dhs.gov/xlibrary/assets/hr\\_5005\\_enr.pdf](http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf).

Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, [http://www.nctc.gov/docs/pl108\\_458.pdf](http://www.nctc.gov/docs/pl108_458.pdf).

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

*National Infrastructure Protection Plan*, 2009, Chapter 4 and Appendices 5a&b, [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

*Information Sharing and the Private Sector*, <http://www.ise.gov/Pages/sharingprivatesector.aspx>

Information Sharing Governance Board, DHS Strategy for Information Sharing, April 18, 2008, [http://www.dhs.gov/xlibrary/assets/dhs\\_information\\_sharing\\_strategy.pdf](http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf).

Presidential Memorandum, *Guidelines and Requirements in Support of the Information Sharing Environment*, December 16, 2005, <http://www.fas.org/sgp/news/2005/12/wh121605-memo.html>.

*The 9/11 Commission Report*, July 22, 2004, Chapter 13, <http://govinfo.library.unt.edu/911/report/index.htm>.

#### **4. Additional Recommended Reading:**

R.A. Best, *Sharing Law Enforcement and Intelligence Information: The Congressional Role*, Congressional Reporting Service, RL 33873, 2007, <http://www.fas.org/sgp/crs/intel/RL33873.pdf>.

*Information Sharing Environment*, [http://itlaw.wikia.com/wiki/Information\\_Sharing\\_Environment](http://itlaw.wikia.com/wiki/Information_Sharing_Environment).

Kshemendra N. Paul (Program Manager, Information Sharing Environment), *Information Sharing Environment: Annual Report to Congress*, July 2010,

[http://www.ise.gov/docs/ISE\\_AR-2010\\_Final\\_2010-07-29.pdf](http://www.ise.gov/docs/ISE_AR-2010_Final_2010-07-29.pdf).

D.C. Piette and J. Radack, *Piercing the 'Historical Mists': The People and Events Behind the Passage of FISA and the Creation of the 'Wall,'* *Stanford Law and Policy Review*, Spring 2006, 261.

Thomas E. McNamara (Program Manager, Information Sharing Environment), *Information Sharing Environment Implementation Plan*, 2006, <http://www.ise.gov/docs/ISE-impplan-200611.pdf>.

The White House, *The National Security Strategy*, May 2010, [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/national\\_security\\_strategy.pdf](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:**

- Understand the following principles or “best practices” 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

M.L. Cohen, *Theory and Principles of Effective Information Sharing*, 2010.

M.L. Cohen, *Information Sharing Best Practices*, 2010.

D. Dörner, *Logic of Failure: Recognizing and Avoiding Error in Complex Situations*, Perseus Books: Cambridge, 1996.

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

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

## **LESSON 4 TOPIC: FRAMEWORK FOR INFORMATION SHARING**

### **1. Lesson Goals/Objectives:**

- Understand that a general framework exists that includes generally-accepted information sharing elements
- Learn that the framework has five dimensions and understand the reasons for each of them:
  - Information Sharing Terminology and Definitions
  - Systems Used to Handle or Control Information Dissemination
  - Senders and Receivers
  - Technology
  - Performance Metrics and Feedback Mechanisms
- Understand that each information sharing partner can be both a sender and a receiver of information, although the primary responsibility for sending out threat information resides with Federal, State, local, tribal, and territorial governments
- Understand that the primary senders of Critical Infrastructure information are the following partners:
  - DHS
  - U.S. Department of Justice (DOJ)/Federal Bureau of Investigation (FBI)
  - Intelligence Community
  - State and Local Fusion Centers
  - Joint Terrorism Tasks Forces located in every State
  - State and Local Emergency Management and Emergency Operations Centers
  - Critical Infrastructure Owners and Operators

Understand that it is imperative that the Department and the critical infrastructure community adopt common definitions for risk-related terminology and make every effort to use these common definitions in written and oral communication within and across the critical infrastructure sectors (DHS Risk Lexicon Working Group or Steering Committee)

### **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?
- What are some of the most commonly used systems for sharing information between the government and industry for purposes of critical infrastructure protection? 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.

### 3. Required Reading:

Textbook: Chapters 7-8.

P. Adriaans and J. V. Benthem (eds.), "Philosophy of Information," in series Gabby, Thagard, and Woods (eds.) *Handbook of the Philosophy of Science*, Elsevier, 2008.

S. Barrett and B. Konsynski, "Inter-Organizational Information Sharing," *MIS Quarterly*, 6: December 1982 Special Issue, 93-105.  
<http://www.jstor.org/stable/248993?seq=1>.

M.L. Cohen, *Information Sharing Framework*.

D. Constant, S. Kiesler, and L. Sproull, "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>.

F.S. Correa Da Silva and J. Agusti-Cullell, *Information Flow and Knowledge Sharing*, Elsevier, 2008.

DHS, DHS Risk Lexicon: 2010 Edition.  
<http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>.

H.L. Lee, K.C. So, and C.S. Tang, "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>.

T.W. Malone, K.R. Grant, F.A. Turbak, S.A. Brobst, and M.D. Cohen, "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:**

- Understand that the major parties involved in critical infrastructure protection information sharing include the following pair-wise groupings of partners:
  - Federal government - Federal government (includes Intelligence Community agencies to non- Intelligence Community Federal agencies)
  - Federal government – State & local, tribal and territorial governments
  - Federal government – Private Sector
  - State and local government – Private Sector (includes Law Enforcement to Private Sector and Fusion Centers to Private Sector)
  - Regional Consortia – Private Sector
  - Private Sector - Private Sector (includes ISACs and Trade Associations to their members)
- Understand that the three most important pair-wise groupings for critical infrastructure protection information sharing are:
  - Federal government – Private Sector
  - State and local Government – Private Sector
  - Federal government – State and local government
- Become familiar with the key organizations that have formed to facilitate critical infrastructure protection information sharing:
  - Sector Coordinating Councils (SCCs)
  - Sector Specific Agencies (SSAs) and Government Coordinating Councils (GCCs)
  - State and Local, Tribal and Territorial - Government Coordinating Council (SLTT-GCC)
  - Critical Infrastructure Partnership Advisory Council (CIPAC)
  - Information Sharing and Analysis Centers (ISACs) and the Information Sharing and Analysis Center Council
  - State and local Fusion Centers
  - Joint Terrorism Task Forces (JTTFs)
  - State and local Emergency Operations Centers (EOCs)
  - DHS/ Intelligence & Analysis
  - DHS/ National Infrastructure Coordination Center (NICC)
  - DHS/Regional Protective Security Advisors (PSAs) and Regional Mission Collaboration Staff
  - DHS/Federal Emergency Management Agency (FEMA)
- Understand that four areas were assessed by DHS as being common benefits Fusion Centers would yield to DHS and state and local authorities:
  - Clearly defined information gathering requirements
  - Improved intelligence analysis and production capabilities
  - Improved information/intelligence sharing and dissemination.
  - Improved prevention, protection, response, and recovery
- Understand that unique benefits of Fusion Centers to DHS include:
  - Improved information flow from state and local entities to DHS

- Improved situational awareness
- Improved access to local officials.
- Consultation on state and local issues
- Access to non-traditional information sources
- Understand what special challenges are 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 CIP 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 special coordination role does the Sector Specific Agency 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?
- Why are the Federal government – Private Sector, State and local government – Private Sector, and Federal government – State and local government the most important pair-wise groupings for sharing critical infrastructure protection 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 protection capabilities, including information sharing with local critical infrastructure protection 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

*A Functional Model for Critical Infrastructure Information Sharing and Analysis*, 2004,  
[http://www.isaccouncil.org/index.php?option=com\\_docman&task=doc\\_view&gid=9&Itemid=208](http://www.isaccouncil.org/index.php?option=com_docman&task=doc_view&gid=9&Itemid=208).

*A Policy Framework for the ISAC Community*, 2004,  
[http://www.isaccouncil.org/index.php?option=com\\_docman&task=doc\\_view&gid=13&Itemid=208](http://www.isaccouncil.org/index.php?option=com_docman&task=doc_view&gid=13&Itemid=208).

DHS, *State and Local Fusion Centers*, September 16, 2009,  
[http://www.dhs.gov/files/programs/gc\\_1156877184684.shtm](http://www.dhs.gov/files/programs/gc_1156877184684.shtm).

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

U.S Government Accountability Office (GAO), *Information Sharing: Federal Agencies Are Sharing Border and Terrorism Information with Local and Tribal Law Enforcement Agencies, but Additional Efforts Are Needed*, GAO-10-41, December 2009.  
<http://www.gao.gov/new.items/d1041.pdf>.

### **4. Additional Recommended Reading:**

Arjen Boin and Denis Smith, "Terrorism and Critical Infrastructures: Implications for Public-Private Crisis Management," *Public Money & Management* 26(5), 2006, 295-304.

U.S. Government Accountability Office (GAO), *Public Transit Security Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach*, GAO-10-895, September 2010, <http://www.gao.gov/new.items/d10895.pdf>.

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

### **5. Initiate Research Paper**

Initiate the term research paper by requiring turn in of 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:**

- Understand how the public-private partnership as implemented by DHS IP performs information sharing with the 18 critical infrastructure sectors
- Understand the role of the SCCs and their Information Sharing Working Groups in the process
- Understand the role of IP's Partnership Programs and Information Sharing (PPIS) Branch in providing the public-private partnership governance rules as well as Secretariat support for the GCCs and SCCs
- Understand the role of the CIPAC in providing *cross sector* information sharing and coordination
- Understand the roles of the 24 x 7 National Infrastructure Coordination Center and the Homeland Security Information Network (HSIN) – Critical Sector (CS) system in operationalizing the information sharing process with the 18 critical infrastructure sectors
- Understand the role of State and Local Fusion Centers and Joint Terrorism Task Forces (JTTFs) in sharing local threat information with critical infrastructure sector entities within their jurisdiction  
Understand that members of the local Joint Terrorism Task Forces (JTTFs), including the FBI, are often the officials who share targeted facility, asset, and system-specific threat information with critical infrastructure owners and operators

### **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 2009 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:**

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

*National Infrastructure Protection Plan*, 2009, Chapter 4 (including page 64) and Appendices 5a&b, [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

*The Role of ISACs in Private/Public Sector CIP*, 2009,  
[http://www.surface-transportation-isac.org/SupDocs/Library/ISAC\\_Products/isac\\_role\\_in\\_cip.pdf](http://www.surface-transportation-isac.org/SupDocs/Library/ISAC_Products/isac_role_in_cip.pdf).

Robert F. Dacey, *Critical Infrastructure Protection: Improving Information Sharing With Infrastructure Sectors*, United States General Accounting Office, 2006.

DHS, “Charter of the Critical Infrastructure Partnership Advisory Council (CIPAC),” 2010,  
[http://www.dhs.gov/xlibrary/assets/cipac/cipac\\_charter.pdf](http://www.dhs.gov/xlibrary/assets/cipac/cipac_charter.pdf).

United States Government Accountability Office, *Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results*, GAO-10-972, 2010.

## **LESSON 7 TOPIC:    INFORMATION SHARING LIFECYCLE**

### **1. Lesson Goals/Objectives:**

- Understand the six phases of the information sharing lifecycle: requirements; collection/storage; analysis; production; dissemination; feedback and update
- Understand that SCCs and critical infrastructure owners and operators have roles to play in the requirements, collection, dissemination, and feedback phases
- Understand that DHS/Intelligence and Analysis is the focal point at DHS for collecting and disseminating Intelligence from the Intelligence Community as well as from DHS Law Enforcement components
- Understand that DHS/Intelligence and Analysis and State & Local Fusion Centers have roles to play in all phases of the information sharing lifecycle for both steady-state and crisis conditions
- Understand that DHS/NICC plays a role in all lifecycle phases for steady-state, incident, and crisis conditions

### **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 that 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 protection?
- 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:**

DHS, *Secretary Napolitano Announces Rail Security Enhancements, Launches Expansion of ‘See Something, Say Something’ Campaign*, 2010,  
[http://www.dhs.gov/ynews/releases/pr\\_1278023105905.shtm](http://www.dhs.gov/ynews/releases/pr_1278023105905.shtm).

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

U.S. Air Force, Requirements Development and Processing,” 1999, [www.e-publishing.af.mil](http://www.e-publishing.af.mil).

## **LESSON 8 TOPIC: INFORMATION SHARING PRODUCTS**

### **1. Lesson Goals/Objectives:**

- Understand that most DHS products are no longer sent out by email but are posted to secure Homeland Security Information Network (HSIN) Portals like the Homeland Security Information Network - Critical Sector (HSIN-CS) Portal
- Understand that all common cross sector products are posted to the HSIN-CS homepage or links thereto and that all sector-specific products are posted to sector-specific HSIN-CS Portals
- Understand that in order to access products on HSIN-CS the subscriber must first be vetted by the critical infrastructure sector to which the subscriber belongs
- Understand that many of the products on HSIN-CS are designated For Official Use Only (FOUO) and can only be shared with those that have a need to know
- Become familiar with 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 & 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
- Understand that other Federal departments such as the Department of Justice have information sharing constructs and systems. For example, DOJ has the Global Justice Information Sharing Initiative; the FBI's National Information Sharing Strategy (2011), and the FBI's InfraGard Program
  - Develop skills in how to develop and share an information product

### **2. Homework:**

Develop a critical infrastructure protection 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)
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 in 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 protection needs of most critical infrastructure owners and operators? If so, why? If not, why not?

### 4. Required Reading:

M.L. Cohen, *I&A Threat Products*, 2010.

M.L. Cohen, *Cyber Threat and Vulnerability Products*, 2010.

FBI InfraGard Program at <http://www.infragard.net/>.

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

Yacov Y. Haimes, "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 9 TOPIC: SHARING OF SENSITIVE AND CLASSIFIED INFORMATION**

### **1. Lesson Goals/Objectives:**

- Understand why so much of Homeland Security information is designated sensitive-but-unclassified or is classified
- Understand the difference in legal status and penalties associated with unauthorized disclosure of classified versus sensitive but unclassified information
- Understand the specific types of sensitive but unclassified (SBU) information that DHS shares such as: For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Chemical Vulnerability Information (CVI), Protected Critical Infrastructure Information (PCII), Safeguards Information(SGI), and Sensitive Security Information (SSI).
- Understand that the private sector also has sensitive information that is usually designated as Proprietary or Business Confidential
- Understand the various levels of classified information: Confidential, Secret, and Top Secret
- Appreciate how sensitive but unclassified and classified information can create barriers to sharing and how these barriers are legally overcome
- Understand how classified information can be redacted or downgraded to lower classification levels to enhance sharing, often referred to as creating a “Tearline”
- Understand the new Information Sharing Environment designation of Controlled Unclassified Information (CUI) and how it systematizes all forms of sensitive but unclassified information

### **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:

M.L. Cohen, *Obama vs. Bush on Classified Information*, 2010.

Executive Order 12958 - Classified National Security Information, as Amended at <http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html>.

Executive Order 13292 - Further Amendment To Executive Order 12958, As Amended, Classified National Security Information, <http://www.fas.org/sgp/bush/eoamend.html>.

Executive Order - Classified National Security Information, 2009, <http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information>.

Executive Order - Controlled Unclassified Information, 2010, <http://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-controlled-unclassified-information>.

J. Warrick, “WikiLeaks Cable Dump Reveals Flaws of State Department's Information-Sharing tool,” Washington Post, December 30, 2010.

## **LESSON 10 TOPIC: SYSTEMS & TOOLS FOR SHARING SENSITIVE AND CLASSIFIED INFORMATION**

### **1. Lesson Goals/Objectives:**

- Understand that there are commonly used systems for sharing SBU \ Controlled Unclassified Information (CUI) with critical infrastructure owners and operators and State and Local homeland security officials: HSIN-CS and US-Computer Emergency Readiness Team (US-CERT) for CI owners and operators and Homeland Security Information Network -Intel\ Homeland Security State and Local Intelligence Community of Interest (HS-SLIC) for State and local homeland security officials
- Understand that there are two commonly used classified systems:
  - Homeland Secure Data Network (HSDN)
  - Homeland Top Secret Network (HTSN) (interoperable with JWICS)
- Understand that there are generally six 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
- Understand that there are strict rules and procedures to be followed for uploading and downloading information from/to electronic media (e.g., USB drives) from DHS systems
- Understand that there are 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
- Understand that not all information sharing takes place through the Internet but occurs through face-to-face SCC and GCC Working Group meetings and peer-to-peer communications through telephony, cell phones, and smart phones.

### **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:**

DHS, *DHS' Efforts to Improve the Homeland Security Information Network*, Office of the Inspector General, 2008, [http://www.dhs.gov/xoig/assets/mgmtrpts/OIG\\_09-07\\_Oct08.pdf](http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_09-07_Oct08.pdf).

DHS, *About the Homeland Security Information Network*, 2010, [http://www.dhs.gov/files/programs/gc\\_1156888108137.shtm](http://www.dhs.gov/files/programs/gc_1156888108137.shtm).

DHS, *Homeland Security State & Local Intelligence Community of Interest (HS SLIC)*, 2010, [http://www.dhs.gov/files/programs/gc\\_1233582654947.shtm](http://www.dhs.gov/files/programs/gc_1233582654947.shtm).

U.S. Government Accountability Office (GAO), *Information Technology: Management Improvements Needed on the Department of Homeland Security's Next Generation Information Sharing System*, GAO-09-40, October 2008, <http://www.gao.gov/new.items/d0940.pdf>.

US-CERT, "Welcome to US-CERT," 2010, <http://www.uscert.gov/index.html>.

## **LESSON 11 TOPIC: STANDARD OPERATING PROCEDURES (SOPs) FOR MAINTAINING CRITICAL INFRASTRUCTURE INFORMATION SHARING PORTALS**

### **1. Lesson Goals/Objectives:**

- Understand that in order for critical infrastructure Information Sharing Portals to be refreshed, maintained, and used by critical infrastructure owners and operators there need to be Standard Operating Procedures (SOPs) for their governance
- Learn that for the sector-specific Portals on HSIN-CS, six basic Standard Operating Procedures are required:
  - Nominating, Vetting and Validation;
  - Data Management Process;
  - Routine Communication;
  - Incident Communication;
  - Alerts, Warnings, and Notifications;
  - Suspicious Activity Reporting
- Understand that the first, second, and fifth SOP above requires Administrative privileges on the portal
- Gain familiarity with a fully worked example of the six Standard Operating Procedures in the Food and Agriculture sector as applied to their FoodSHIELD portal (SOPs are on CD)
- Understand that since each critical infrastructure SCC owns its sector-specific Portal, it is primarily responsible for developing and resourcing the SOPs. Technical assistance is available from DHS/IP
- Understand that the six basic Standard Operating Procedures are considered the minimum necessary and that each SCC is free to develop additional Standard Operating Procedures to meet the sector's needs
- Understand that while the critical infrastructure Sector Coordinating Councils are encouraged to use the free networking infrastructure of HSIN-CS, the SCCs are free to develop and/or use other information sharing platforms to meet their sector's needs
- Understand that the new Nationwide Suspicious Activity Reporting (SAR) Initiative contains a Federated search tool to help "connect the dots" from SARs reported by multiple Federal agencies that may have originated with critical infrastructure owners and operators

### **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”?

### **3. Required Reading:**

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:**

- Understand that in addition to HSIN-CS and its sector-specific Portals, there are a variety of other information sharing mechanisms used to support the public-private partnership and to share information with all parties to the partnership. The most commonly used other information sharing mechanisms include:
  - DHS email
  - Smart phones/Personal Digital Assistants
  - Teleconferences
  - Webinars
  - Chat on HSIN-CS
  - Video Teleconferences (VTCs)
  - DHS Blogs (<http://blog.dhs.gov> )
  - DHS Protective Security Advisors (PSAs)
  - Conferences, Summits, Workshops
- Understand that the Department of Justice also has information sharing mechanisms in which the private sector can participate: Law Enforcement Online (LEO); Regional Information Sharing System, and the secure InfraGard web site just to name a few
- Learn that emerging technology on the horizon includes the Secure Mobile Environment – Portable Electronic Devices (SME-PEDs) for classified voice and data sharing
- Understand that while the new social networking media are not a secure means for sharing terrorist-related information, they may be useful for natural disaster related information sharing
- Understand that all Sector Coordinating Council members and vetted critical infrastructure owners and operators are permitted to subscribe to the Government Emergency Telecommunications Service (GETS) and the Wireless Priority Service (WPS)

### **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?

- On other hand, what would be the benefits of using social networking media to communicate during or in the wake of 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?

### **3. Required Reading:**

M. L. Cohen, *The Two Sides of Information Exchange: Protection and Sharing*, 2008.

DHS, "The Blog @ Homeland Security," 2010,  
<http://blog.dhs.gov/search/label/aviation%20security>.

Department of Homeland Security, "Example Webinar: The Evolving Threat: What You Can Do," 2010, [http://www.fbiic.gov/public/2010/nov/DHS\\_Webinar\\_Invite.pdf](http://www.fbiic.gov/public/2010/nov/DHS_Webinar_Invite.pdf).

Department of Homeland Security, 2010, "Jabber (Chat)."  
<https://im.hsin.gov/jmweb/dynamic/chat.html#a>.

DHS, "Regional Directors and Protective Security Advisors,"  
[http://www.dhs.gov/files/programs/gc\\_1265310793722.shtm](http://www.dhs.gov/files/programs/gc_1265310793722.shtm).

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

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

L-3 Guardian<sup>®</sup> Secure Mobile Environment Portable Electronic Device (SME PED), 2010,  
[http://www.l-3com.com/cs-east/ia/smeped/ie\\_ia\\_smeped.shtml](http://www.l-3com.com/cs-east/ia/smeped/ie_ia_smeped.shtml).

LEO: <http://www.fbi.gov/about-us/cjis/leo>.

National Communications Systems, "Government Emergency Telecommunications Service," 2010, <http://gets.ncs.gov/>.

National Communications Systems, "Welcome to the Wireless Priority Service (WPS) Website!" 2010, <http://wps.ncs.gov/>.

Regional Information Sharing System at <http://www.riss.net/>.

### **4. Additional Recommended Reading:**

Louise K. Comfort, "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](http://www.cdm.pitt.edu/Portals/2/PDF/Publications/RISK_AND_RESILIENCE.pdf).

DHS, "2011 Chemical Sector Security Summit," 2010.  
[http://www.dhs.gov/files/programs/gc\\_1176736485793.shtm](http://www.dhs.gov/files/programs/gc_1176736485793.shtm)

T.L. Dinh and A.V. Nguyen-Ngoc, "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://delivery.acm.org/10.1145/1860000/1852640/p147-dinh.pdf?key1=1852640&key2=2508440921&coll=DL&dl=ACM&CFID=115374370&CFTOKEN=60447038>.

P.H. Longstaff, "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](http://pirp.harvard.edu/pubs_pdf/longsta/longsta-p05-3.pdf).

## LESSON 13 TOPIC: PREPARATION FOR INFORMATION SHARING EXERCISE

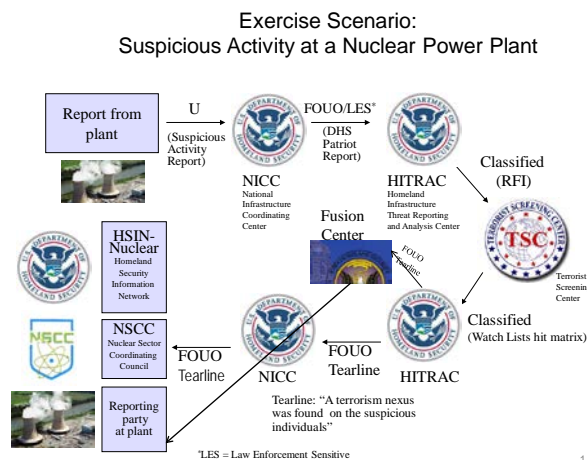
### 1. Lesson Goals/Objectives:

- Make all preparations and lay the foundation for participation in an exercise the following week, to include:
  - Understanding a specific and concrete critical infrastructure threat situation
  - Understanding group roles in the scenario in which each group corresponds to a government or critical infrastructure node in today's networked information sharing environment
- Gain insight into a how the sharing of a SAR can result in value-added threat information being provided back to the submitting critical infrastructure owner and operator and to the critical infrastructure sector as a whole, thereby demonstrating the value of two-way information sharing

### 2. Exercise Scenario:

The scenario consists of the detection of pre-operational terrorist surveillance at a nuclear power plant, the apprehension of the suspected terrorists, the submittal of a Suspicious Activity Report to DHS<sup>1</sup>, the screening and confirmation by the Terror Screening Center (TSC) that the suspected terrorists are *known* terrorists, and the dissemination of that sensitive information back to the nuclear power plant Suspicious Activity Report submitter, to the leadership of the Nuclear Sector Coordinating Council (NSCC), and to all security managers at nuclear power plants. See the information flow in Figure 1.

Figure 1.



<sup>1</sup> Today nuclear power plant SARs are submitted to the U.S. Nuclear Regulatory Commission. However, the transition of SAR submissions from NRC to DHS is under discussion within the Nuclear Sector Coordinating Council (NSCC).

The class will assemble into groups corresponding to each entity or organization shown in the figure. The groups are as follows:

- Security manager at surveilled nuclear power plant (NPP)
- DHS/ National Infrastructure Coordination Center
- DHS/ Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)
- Terror Screening Center
- State Fusion Center
- National Institute of Standards and Technology (NIST)
- Leadership of the Nuclear Sector Coordinating Council
- Security Managers at other nuclear power plants

See the Notes View of the PowerPoint presentation entitled “Information Sharing Exercise – Nuclear Power Plant Threat Scenario” for the script for the moderator and for each group. Each group should feel free to modify or enhance the script as it deems appropriate during the preparation sessions for the exercise. In particular, while not requiring the Nuclear Regulatory Commission (NRC), FBI, and Local law enforcement to be included in the exercise design, the instructor may allow them to be added at the option of the learners if only in the form of simulated message injects.

### **3. Exercise Play**

A moderator (which could be the instructor) will use the script in the PowerPoint presentation to guide the exercise play. The exercise can be conducted either as a Tabletop (TTX) or as computer lab information sharing event in which each group is assigned to a workstation and there is an ability to project each workstation's screen onto a large wall display (e.g., a plasma TV screen). In the case of the computer lab version, any information sharing tools that are available may be used. However, in selecting the tools the groups should either acknowledge their IT security weaknesses or should employ more secure IT tools (e.g., eDRM).

### **4. Discussion Topics:**

- [There is no discussion due to exercise preparations]

### **5. Required Reading:**

M.L. Cohen, “Suspicious Activity at a Nuclear Power Plant,” 2008.

M.L. Cohen, *Information Sharing Scenario – Nuclear Power Threat Scenario*, 2008.

Department of Homeland Security, CIPAC/Nuclear Sector, 2010,  
<http://www.dhs.gov/xlibrary/assets/cipac/cipac-annual-2010.pdf> p. 40 and after.

MITRE Cross-Boundary Information Sharing (XBIS) Lab, 2010,  
<http://www.mitre.org/tech/xbis/>.

## **LESSON 14 TOPIC: INFORMATION SHARING EXERCISE**

### **1. Lesson Goals/Objectives:**

- Experience the look-and-feel of a realistic information sharing threat scenario
- Learn to appreciate the different roles and perspectives of the different critical infrastructure and government players
- Learn the specifics of one particular critical infrastructure information sharing node
- Gain insight into how the fusion of shared information can lead to better preparation for a terrorist attack, including better protection of critical infrastructure assets

### **2. Discussion Topics:**

For the class session following the day of the exercise, the class should conduct a “Hot Wash” to identify information sharing lessons learned from the exercise.

### **3. Required Reading:**

M.L. Cohen, “Suspicious Activity at a Nuclear Power Plant,” 2008.

M.L. Cohen, “Information Sharing Scenario – Nuclear Power Threat Scenario,” 2008.

## **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 6 – 10 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 for the same reasons as above