Chemical Sector Training Resources Guide

March 2012

Homeland Security

Table of Contents

Introduction..... 1

Organizations
- Federal Emergency Management Agency 1
- National Protection and Programs Directorate 3
  - Office of Infrastructure Protection..... 3
  - Cyber Security and Communications 4
- Transportation Security Administration 5
  - Transportation Sector Network Management..... 5

Course Code Key 6

Selected Courses by Category 7
- National Incident Management System 7
- National Response Framework 7
- Security Awareness 8
- Terrorist Acts and Weapons of Mass Destruction 12
- Hazardous Materials 13
- First Responders 13
- Exercises 14
- Hazard Mitigation 16
- Emergency Response 17
- Business Planning 18
- Cybersecurity – Information Security 19
- Cybersecurity – Control Systems 21

List of Acronyms 24

Courses Alphabetized by Category 26

National Protection and Programs Directorate

Office of Infrastructure Protection

The Office of Infrastructure Protection (IP) leads the coordinated national effort to reduce risk to the Nation's critical infrastructure. IP facilitates the identification, prioritization, coordination, and protection of critical infrastructure in support of Federal, State, local, tribal, and territorial governments, as well as the private sector and international entities. IP enhances critical infrastructure-related protective and response capabilities under the National Response Framework, to provide operational support to government and private entities in response to significant threats and incidents.

National infrastructure is divided into 18 distinct critical infrastructure sectors, and coordination of critical infrastructure protection responsibilities for those sectors is assigned to select Federal agencies, designated as Sector-Specific Agencies (SSAs). The Chemical SSA is one of six sectors assigned to IP in the National Protection and Programs Directorate.

The SSA is the primary Federal entity responsible for coordinating the unified effort of the public and private sectors to protect against and mitigate the effects of natural or manmade events against the Chemical Sector. The SSA acts as a liaison between the private sector, through the Sector Coordinating Council (SCC), and the public sector, through the Government Coordinating Council (GCC). The Chemical SSA has collaborated with private and public sector partners to develop a wide range of voluntary programs in an effort to lower the security risk in the Chemical Sector and provide easy-to-use accessible tools. Programs cover a range of free activities from an on-line basic chemical security awareness training program for all chemical facility employees to facilitated tabletop exercises for facility security officers and their local emergency responders. (Chemical Sector Training & Resources Web Site: **http://www.dhs.gov/chem-voluntary-resources)**.

IP also maintains a catalogue of training programs for State, local, and private sector entities specifically designed to develop awareness of terrorist threats to critical infrastructure and educate participants on strategies for detecting and mitigating these threats. Training complements other efforts to protect critical infrastructure sites by developing the capabilities of the facility security officials to identify, detect, and prevent intentional attacks. These training courses are coordinated through the State Homeland Security Officials and State training offices on an annual basis. Past courses have included:

- Private Sector Counterterrorism Awareness Workshop
- Bombing Prevention Workshop
- Improvised Explosive Device (IED) Awareness/Bomb Threat Management Workshop
- IED Search Procedures
- Soft Target Awareness Course

- Protective Measures Course
- Surveillance Detection Training

Descriptions of these courses and course contact information are listed in the *Security Awareness* section of this guide (pages 8-11).

A primary focus of IP is to develop and sustain strategic relationships and information sharing with owners and operators of the Nation's critical infrastructure. IP developed a seminar series designed to educate participants about the linkages between the Critical Infrastructure and Key Resources Support Annex of the National Response Framework and the National Infrastructure Protection Plan – two documents used in responding to and preparing for disasters. The seminars provide critical infrastructure owners and operators and other partners with current information about the tools, latest trends, issues, and best practices in infrastructure protection. Past Webinar topics have included:

- The Effective Use and Visualization of CIKR Data
- IED Awareness
- Engaged Partnership for Disaster Response
- The Active Shooter Awareness Virtual Roundtable

If you are interested in receiving information on the latest seminar series or to access archived webinars, please visit the CIKR Learning Series Web site:
http://www.dhs.gov/files/programs/gc_1231165582452.shtm

Cyber Security & Communications

The National Cybersecurity Division (NCSD) within the Office of Cybersecurity & Communications (CS&C) serves as the national focal point for cybersecurity and collaborates with numerous components within DHS to provide all sector partners with cybersecurity resources, cross-sector information-sharing support, and technical assistance necessary to best prepare for and respond to cyber events. As part of that effort, NCSD develops approaches and methodologies to assist organizations with protecting critical infrastructure. NCSD offers several courses on control systems cybersecurity through the Control Systems Security Program (CSSP).

Control Systems Security Program

Web Site: http://www.uscert.gov/control_systems/

The Control Systems Security Program (CSSP) was established by DHS in 2005 with the mission to reduce Industrial Control System (ICS) risks across all critical infrastructure. To accomplish this mission, CSSP implements several initiatives to reduce the likelihood of success and decrease the severity of a cyber attack against critical infrastructure assets. To address specific concerns of the public and private sectors, CSSP developed a series of risk management activities including:

- Analysis of malware and the impact to the control systems community;

COURSE CODE KEY

COURSE CODE KEY		
Provider	**Course Code**	**Contact Information**
FEMA EMI Independent Study Program	IS – ###	800-238-3358 Independent.Study@dhs.gov
FEMA National Training and Education Division		
• Rural Domestic Preparedness Consortium	AWR – ### PER – ### MGT – ###	Main Office: 877-855-7372 Info@ruraltraining.org
• Texas Engineering Extension Service WMD Campus	AWR – ###	877-833-9638 Terrorism.awareness@teexmail.tamu.edu
• National Fire Academy	Q ###	888-834-6976 Help@nfa.plateau.com
• Department of Energy Emergency Operations Training Academy	CIP ###	505-842-7110 Eota@eota.energy.gov
FEMA Private Sector Office	FEMA Private Sector Office	FEMA-Private-Sector@dhs.gov
Chemical Sector-Specific Agency	Chemical SSA	ChemicalSector@dhs.gov
Office for Bombing Prevention	OBP	OBP@dhs.gov
Control Systems Security Program	CSSP	CSSP@dhs.gov
Transportation Security Administration	TSA	FreightRailSecurity@dhs.gov HighwaySecurity@dhs.gov PipelineSecurity@dhs.gov

SELECTED COURSES BY CATEGORY

National Incident Management System

National Incident Management System, An Introduction (IS-700.A)
This two-day course will describe to participants the components of a multi-agency coordination system and establish relationships between all elements of the system. After taking the course, students should be able to:

- Define multi-agency coordination at the Federal, State, and local levels of government.
- Identify each agency involved in incident-management activities to ensure appropriate situational awareness and resources status information is shared through multi-agency coordination.
- Identify typical priorities established between elements of the multi-agency coordination system.
- Define key terms related to multi-agency coordination systems.
- Describe the process of acquiring and allocating resources required by incident-management personnel in relationship to the entire multi-agency coordination system.
- Identify typical future resource requirements for the entire multi-agency coordination system.
- Identify potential coordination and policy issues arising from an incident relative to the entire multi-agency coordination system.

Online at: http://training.fema.gov/EMIWeb/IS/is700a.asp

National Response Framework

National Response Framework, An Introduction (IS-800.B)

This course is intended for government executives, private sector and nongovernmental organizations (NGO) leaders, and emergency-management practitioners. This includes senior elected and appointed leaders, such as Federal department or agency heads, State Governors, mayors, tribal leaders, and city or county officials who have a responsibility to provide for effective response. This course introduces participants to the concepts and principles for the National Response Framework (NRF). At the end of this course, students should be able to describe the following:

- Purpose of the NRF;
- Response doctrine established by the NRF;

Bombing Prevention Workshop (OBP)

This one-day workshop is intended for regional level public and private stakeholders and planners from emergency management, security and law enforcement and designed to enhance the effectiveness in managing a bombing incident. This workshop reviews the current development of strategies and brings together best practices from regions across multiple localities, disciplines and levels of government. Participants will work together in small groups on critical thought, problem solving and decision making actions that reduce vulnerability and mitigate the risk of terrorist IED attacks. The guided scenario discussion establishes the foundation for the stakeholders within the region to implement a Bombing Prevention Plan. This workshop can accommodate up to 50 participants.

To request training, contact the DHS Office for Bombing Prevention at OBP@dhs.gov.

Hazmat Motor Carrier Security Self Assessment Training Program (TSA)

This program was developed as a cooperative effort between the U.S. Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA), the DOT Federal Motor Carrier Safety Administration (FMCSA), and TSA. The voluntary training program addresses the requirements contained in 49 Code of Federal Regulations (CFR), Part 172.802, which requires motor carriers that transport placarded amounts of hazardous materials to develop a plan that adequately addresses security risks related to the transportation of hazardous materials. It is designed to provide the necessary knowledge and tools to conduct an effective assessment of operations. It also offers security actions to consider when managing the risks related to personnel security, unauthorized access, and en route security. Once the assessment has been conducted and security actions have been considered, the security plan can be put in place.

This voluntary training program is intended for hazmat motor carrier security managers, drivers, and any other personnel involved in the transportation of hazardous materials. The training is available at http://www.tsa.gov/what_we_do/tsnm/highway/self_training.shtm. The training is also available on CD-ROM by emailing TSA at HighwaySecurity@dhs.gov.

IED Awareness/Bomb Threat Management (OBP)

IED attacks remain the primary tactic for bombers, terrorists and criminals seeking relatively uncomplicated, inexpensive means for inflicting mass casualties and maximum damage. This four-hour presentation is designed to enhance and strengthen the participant's knowledge, skills, and abilities in relation to the threat of IEDs. The information presented outlines specific safeties associated with Bomb Threat Management dealing with IED awareness, explosive incidents and bombing prevention. This workshop is designed to provide two four-hour sessions, morning and afternoon, with 50 participants for each session.

To request training, contact the DHS Office for Bombing Prevention at OBP@dhs.gov.

IED Search Procedures (OBP)

This 8-hour workshop of lecture and practical exercises is designed to support special security events and is geared toward security personnel and facility managers of sites hosting any event that requires increased security preparedness. The information provided during the workshop focuses on general safeties used for specialized search and explosive sweeps and can be tailored to meet the needs required in supporting any special security event. The course can accommodate 25 participants.

counterterrorism awareness and prevention actions that reduce vulnerability and mitigate the risk of domestic terrorist attacks. This workshop can accommodate 100 to 250 participants.

To request training, contact the DHS Office for Bombing Prevention at OBP@dhs.gov.

Protective Measures Course (OBP)

This two-day course is designed to enhance commercial sector individual and organizational awareness on how to devalue, detect, deter, and defend facilities from terrorism, providing the knowledge and skills necessary in understanding common vulnerabilities and employing effective protective measures. The course includes lessons learned and industry best practices in mitigating terrorists' attacks. It serves as a follow-up to the Soft Target Awareness Course, focusing more on implementation than awareness. This course can accommodate 35 participants.

To request training, contact the DHS Office for Bombing Prevention at OBP@dhs.gov.

Soft Target Awareness Course (OBP)

This Course is designed to enhance individual and organizational awareness on terrorism and help facilitate information sharing. Commercial infrastructure facility managers, supervisors, operators, and security staff learn to be proactive and better understand their roles in deterring, detecting, and defending their facilities from terrorism. Participants choose from five focus areas within the commercial facilities sector according to their specific affiliation: Stadiums and Arenas; Places of Worship; Education; Malls and Shopping Centers; and Large Buildings, Hotels and Medical Facilities. Each of these focus areas is comprised of a four-hour session of combined informal lecture and capstone guided discussions. Each session can accommodate 35 participants or can be modified for one general session for up to 175 participants.

To request training, contact the DHS Office for Bombing Prevention at OBP@dhs.gov.

Surveillance Detection Training for Commercial Infrastructure Operators and Security Staff (OBP)

This three-day course explains how protective measures can be applied to detect and deter potential threats to critical infrastructure, as well as the fundamentals for detecting surveillance activity. Students apply skills such as vulnerability and red zone analysis, surveillance detection, and observation and reporting during practical exercises. The course is designed for commercial infrastructure operators and security staff of critical facilities. This course can accommodate 25 participants.

To request training, contact the DHS Office for Bombing Prevention at OBP@dhs.gov.

Vehicle Bomb Search Methods (CIP 110 DW)

This interactive course provides security personnel and others with the basics of access point and parked vehicle bomb search methods. There is also a historical perspective that explains various significant bombings in the United States and abroad. Several games are incorporated to enhance the learning experience and provide a review of the lessons. An interactive exercise provides practice of the learned search techniques.

Register for online courses at: http://eota.doeal.gov/eota. Once registered, view and select courses by clicking on the "courses" button at the top of the page. An "Add New Courses" how-to guide is also available by emailing eota@eota.energy.gov

Workplace Security Awareness (IS-906)

This self-paced course provides guidance to individuals and organizations on how to improve security in the workplace. No workplace – be it an office building, construction site, factory floor, or retail store – is immune from security threats. Employees are often the target of these threats as well as the organization's first line of defense against them. Threats endanger the confidentiality, integrity, and security of your workplace, as well as your virtual workplace and computer systems. This course presents information on how employees can contribute to your organization's security.

Upon completing this one-hour course, employees will be better equipped to:

- Identify potential risks to workplace security;
- Describe measures for improving workplace security; and
- Determine the actions to take in response to a security situation.

Online at: http://training.fema.gov/EMIWeb/IS/IS906.asp

Terrorist Acts and Weapons of Mass Destruction

Terrorism and Weapons of Mass Destruction (WMD) Awareness in the Workplace (AWR-187-W)

This Web-based training course will prepare students to successfully recognize, report, and react to potential terrorist incidents. Students will develop a broad understanding of terrorism to include a definition of terrorism as well as examples of terrorist groups and targets. Students will also gain insight into the importance of protecting private sector resources through awareness-level training. Finally, students will gain knowledge of various WMDs, relay indicators of potential terrorist activity, and outline actions to be taken in the event of a potential terrorist attack.

Go to http://ruraltraining.org/training/online and select this course title from the list. Follow the directions provided to register for this course.

Weapons of Mass Destruction (WMD): Training (CIP 300 DC)

This CD-ROM series is comprised of four separate training programs designed to support WMD training activities at the State and local level. The programs include: Incident Commander and Staff; HAZMAT – First Responder; Hospital and EMS – First Responder; and General Education. The General Education module is divided into the following four training areas:

- **Terrorism:** Learn about the characteristics of terrorism, terrorist WMD attack characteristics, indicators of a WMD attack, and a WMD terrorism incident versus a hazardous material incident.

- **WMD Agent Properties:** Learn about explosives effects, chemical agent effects, and biological agent effects.

- **Protection Procedures:** Learn about detection and identification equipment, personal protective equipment, and safety procedures.

- **Response Actions:** Learn about the planning process for addressing WMD, the decontamination process, and the role of 911 operators and dispatchers.

Register for online courses at: http://eota.doeal.gov/eota. Once registered, view and select courses by clicking on the "courses" button at the top of the page. Follow the instructions provided to request the CD-ROM series for this course. An "Add New Courses" how-to guide is also available by emailing eota@eota.energy.gov.

Hazardous Materials

An Introduction to Hazardous Materials (IS-5.A)

This Independent Study course is intended to provide a general introduction to hazardous materials. No prior knowledge of the subject is required or assumed. At the end of the course, the participant should be able to:

- Explain the roles of Federal, State, local, and tribal governments in reducing hazardous materials risks through Health and Environmental Regulations.

- Discuss the two major hazardous materials identification systems used within the United States.

- Identify possible terrorist's targets of opportunities in the use of toxic industrial chemicals (TIC) as Weapons of Mass Destruction (WMD).

- Identify locations where hazardous materials are commonly found and how to determine their potential health effects.

- Identify steps individuals and communities can take to protect themselves during a hazardous materials release.

Online at: http://training.fema.gov/EMIWeb/IS/is5.asp

First Responders

Emergency Response to Terrorism: Self-Study (Q 534)

This self-study course is designed to provide the basic awareness training to prepare first-responders to respond safely and effectively to potential terrorist incidents. Students who successfully complete the exam will be eligible for a National Fire Academy Certificate of Training.

Register and take this course online at: http://www.nfaonline.dhs.gov/browse/index.shtm

Rail Car Incident Response (AWR-147)

This course has been developed to educate rural emergency responders on freight rail car incidents involving hazardous materials. Through this course, participants will gain an understanding of potential hazards at a train derailment, the properties of specific chemicals, and various incident control, confinement, and containment mitigation techniques. In addition, participants will learn about basic rail car design and construction features as well as damage-assessment strategies to help interpret damage to the rail cars in the event of an incident. Upon completion of this course, participants should be better prepared to respond to a freight rail car incident without endangering the health and safety of the responders and the environment.

To view a schedule of current training and locations go to: http://www.ruraltraining.org/training. Choose this course if it is available at a convenient time and location and follow the registration instructions provided. If you would like to request a course delivery in your area, click on the "Request a Course" button at the top of the page and follow the instructions provided.

WMD/Terrorism Awareness for Emergency Responders (AWR-160)

This course provides participants with a basic knowledge of hazardous materials, WMDs, and response actions to incidents involving these materials. This course also introduces topics such as the Emergency Response Guide, NFPA 704 marking system, and more. The course is NFPA 472 compliant and meets the requirements for Hazardous Materials Awareness Level training.

To register, go to: www.teexwmdcampus.com. Once registered, click on "public catalog" from the left hand menu and select this course from the list.

Exercises

An Introduction to Exercises (IS-120.A)

This course builds a foundation for subsequent exercise courses, which provide the specifics of the Homeland Security Exercise and Evaluation Program (HSEEP) and the National Standard Exercise Curriculum (NSEC). This class will introduce the basics of emergency-management exercises, including:

- Managing an exercise program
- Designing and developing an exercise
- Conducting an exercise
- Evaluating an exercise
- Developing and implementing an improvement plan

Online at: http://training.fema.gov/EMIWeb/IS/IS120a.asp

Active Shooter & Workplace Violence Tabletop Exercise (TTX) and Resources (Chemical SSA)

The Office of Infrastructure Protection's (IP) Sector-Specific Agency Executive Management Office (SSA EMO) has developed the Dealing with Workplace Violence Tabletop Exercise (TTX) that

focuses on an active-shooter situation in the workplace. The TTX is broken up in three modules: the pre-incident phase, including recognizing potential warning signs of workplace violence; the incident and response phase; and the assessment phase, which occurs after the incident has concluded. The TTX will focus discussion on how to limit escalation and reduce the threat of violent behavior, but in the event that an incident does occur, it also addresses how facilities can work with their employees, and public and private partners to ensure they are prepared and able to recover from an event as quickly as possible.

For a CD of the TTX materials and resources, send an e-mail request to ChemicalSector@dhs.gov.

Emergency Planning Exercises for Your Organization (FEMA Private Sector Office)
FEMA is now providing a series of Tabletop Exercise presentations as a tool to advance an organization's continuity, preparedness and resiliency. Each exercise includes a realistic disaster scenario and facilitates a discussion of how your organization would plan, protect, respond and recover. Each includes full instructor's notes so you can gather a facilitator and a team or participants, and self-facilitate the exercise internally.

Two exercises are currently available and draw on the Federal government's National Planning Scenarios:

- FEMA Hurricane Tabletop Exercise 2010
- FEMA Chemical Accident Tabletop Exercise 2010

Also included in the materials are simulated TV news videos suggesting exercise-focused local reporting of the disasters. This feature adds a sense of realism and helps to motivate interactive discussion. The exercises typically take 2-4 hours from start to finish and can be customized where noted in the facilitator's notes to meet your needs. These exercises are structured on the Tabletop Exercise Design curriculum developed by FEMA's Emergency Management Institute, as well as other FEMA/DHS training reference materials.

All exercise materials are free and available to download at:
http://www.fema.gov/privatesector/exercises.shtm

Exercise Evaluation and Improvement Planning (IS-130)
This course introduces the basics of emergency-management exercise evaluation and improvement planning. It also builds a foundation for exercise evaluation concepts as identified in the Homeland Security Exercise and Evaluation Program.

Online at: http://training.fema.gov/EMIWeb/IS/IS130.asp

Infrastructure Protection Sector-Specific Tabletop Exercise Program (IP-SSTEP) Chemical Sector Tabletop Exercise (TTX) (Chemical SSA)
The IP-SSTEP Chemical Sector TTX is an unclassified and adaptable exercise developed for the purpose of creating an opportunity for critical infrastructure stakeholders and their public safety partners to address gaps, threats, issues, and concerns identified in previous exercises and their after-action processes affecting the Chemical Sector. The IP-SSTEP Chemical Sector TTX allows participants the opportunity to gain an understanding of issues faced prior to, during, and after a terrorist threat/attack and the coordination with other entities, both private and government,

regarding their facility. It also contains everything needed to conduct a Homeland Security Exercise and Evaluation Program (HSEEP) compliant TTX.

For a CD of the IP-SSTEP Chemical Sector TTX materials, send an e-mail request to ChemicalSector@dhs.gov.

Major Earthquake Tabletop Exercise (Chemical SSA)

The Major Earthquake Tabletop Exercise (TTX) is an opportunity for critical infrastructure owners and operators – and their public safety partners – to identify and examine the issues and capability gaps they are likely to face in responding to and recovering from a major earthquake. The TTX provides exercise participants with the opportunity to examine key issues through a series of facilitated discussions designed to simulate information sharing and coordination activities between owners and operators, first responders, and relevant stakeholders during an incident. The TTX contains everything needed to conduct a Homeland Security Exercise and Evaluation Program (HSEEP) compliant TTX.

For a CD of the Major Earthquake Tabletop Exercise materials, send an e-mail request to ChemicalSector@dhs.gov.

Security Seminar & Exercise Series with Chemical Industry Stakeholders (Chemical SSA)

This is a collaborative effort between the DHS Chemical SSA and industry stakeholders such as State chemical industry councils, State homeland security offices, industry trade associations and State emergency management agencies. The intent of the program is to foster communication between facilities and their local emergency response teams by encouraging representatives to share their insight, knowledge, and experiences during a facilitated tabletop exercise. The exercise is catered towards the specific interests of the organizing entity and can include a wide variety of topics and security scenarios such as an active shooter, a hostage situation, or work stoppage due to a suspicious package.

For more information on this program or current dates and locations of scheduled programs, e-mail ChemicalSector@dhs.gov.

Hazard Mitigation

Introduction to Hazard Mitigation (IS-393.A)

As the costs of disasters continue to rise, governments and ordinary citizens must find ways to reduce risks to our communities. As communities plan for new development and improvements to existing infrastructure, mitigation can and should be an important component of the planning effort. This means taking action to reduce or eliminate long-term risk from hazards and their effects. This course provides an introduction to mitigation for those who are new to emergency management or mitigation.

Online at: http://training.fema.gov/EMIWeb/IS/IS393a.asp

Emergency Response

Active Shooter, What You Can Do (IS-907)

An active shooter is an individual actively engaged in killing or attempting to kill people in a confined and other populated area. In most cases, active shooters use firearms and there is no pattern or method to their selection of victims. Active shooter situations are unpredictable and evolve quickly. All employees can help prevent and prepare for potential active shooter situations. This course provides guidance to individuals, including managers and employees, so that they can prepare to respond to an active shooter situation.

Upon completing this course, the participant will be able to:

- Describe appropriate actions to take when confronted with an active shooter and responding law enforcement officials;
- Recognize potential indicators of workplace violence;
- Identify actions to prevent and prepare for potential active shooter incidents; and
- Describe how to manage the consequences of an active shooter incident.

Online at: http://training.fema.gov/EMIWeb/IS/IS907.asp

Are You Ready? An In-depth Guide to Citizen Preparedness (IS-22)

"An In-Depth Guide to Citizen Preparedness" has been designed to help the citizens of this Nation learn how to protect themselves and their families against all types of hazards. The focus of the content is on how to develop, practice, and maintain emergency plans that reflect what must be done before, during, and after a disaster to protect people and their property.

Online at: http://training.fema.gov/EMIWeb/IS/IS22.asp

Chemical Facility Security: Best practices Guide for an Active Shooter Incident (Chemical SSA)

This booklet draws upon best practices and findings from tabletop exercises to present key guidance for chemical facility planning and training, and pose specific questions that an effective active shooter response and recovery plan will answer. It is designed to help both chemical facility management and employees prepare and respond by designating roles and needed actions.

To request a copy of this booklet, e-mail ChemicalSector@dhs.gov.

Emergency Response: Strengthening Cooperative Efforts among Public Safety and Private Sector Entities (PER-280)

This eight-hour performance-level course brings the community together to strengthen collective emergency-management capabilities within the context of critical-infrastructure disasters. Its purpose includes:

- Foster information-sharing and sustainable partnerships among private and public sector groups.

- Clarify private and public sector roles and responsibilities within the National Strategy for Homeland Security.

- Develop strategies for mitigating, preparing for, responding to, and recovering from disasters within a national framework.

To view a schedule of current training and locations go to: http://www.ruraltraining.org/training. Choose this course if it is available at a convenient time and location and follow the registration instructions provided. If you would like to request a course delivery in your area, click on the "Request a Course" button at the top of the page and follow the instructions provided.

Get Ready: Prepare, Plan, and Stay Informed

Emergencies can range from inconvenient to devastating. But you can take some simple preparedness steps in advance to minimize the impact to you, your family, or your business. This Web site shows you how by helping you prepare an emergency supply kit, make an emergency plan, and informing you about different types of emergencies and their appropriate responses. Taking these simple steps can make a big difference.

Information is available online at: http://www.ready.gov

Business Planning

Business Continuity and Emergency Management (MGT-381)

This eight-hour management-level course is designed to prepare small and large businesses to effectively plan for continuing operations before, during, and after emergencies of all types. This seminar strives to teach executive-level managers and small-business owners how to develop a comprehensive and effective business continuity plan from start to finish.

Prerequisites: AWR-187-W, Terrorism and WMD Awareness in the Workplace (see page 10).

To view a schedule of current training and locations go to: http://www.ruraltraining.org/training. Choose this course if it is available at a convenient time and location and follow the registration instructions provided. If you would like to request a course delivery in your area, click on the "Request a Course" button at the top of the page and follow the instructions provided.

Business Information Continuity (AWR-176-W)

This course will train business managers to respond to varying threats that might impact their organization's access to information. This course provides requisite background theory and recommended best practices needed by managers to keep their offices running during incidents of different types. Course topics include:

- Introduction to Business Information Continuity
- Managing a Business Information Continuity Plan

- Technical Vulnerabilities and Controls
- Legal concerns
- Implementing a Business Information continuity Plan

Upon completion of the course, participants may request a certificate of completion provided by DHS FEMA.

To register, go to: www.teexwmdcampus.com. Once registered, click on "public catalog" from the left hand menu and select this course from the list.

Protecting Your Home or Small Business from Disaster (IS-394.A)

The purpose of this course is to provide a foundation of knowledge, in a non-technical format, that will enable participants to:

- Describe different types of natural disasters.
- Describe hazards that pose a risk to their home or small business.
- Explain how protective measures can reduce or eliminate long-term risks to their home and personal property from hazards and their effects.
- Explain how protective measures for small businesses secure people, business property, and building structures and prevent business loss from a natural disaster.

Online at: http://training.fema.gov/EMIWeb/IS/IS394a.asp

Cybersecurity – Information Security

Cyber Incident Analysis and Report (AWR-169-W)

This is a high-level course intended for network administrators, management, or information assurance professionals interested in keeping their systems safe from intrusion, as well as learning how to track incidents when they happen. Participants will be presented with real-world examples and scenarios to help provide knowledge, understanding, and capacity for effective cyber incident analysis and response. Topics covered include:

- Introduction to incident management
- Incident preparation
- Incident detection and analysis
- Containment, eradication, and recovery
- Proactive and incident cyber services

Upon completion of the course, participants may request a certificate of completion provided by DHS FEMA.

To register, go to: www.teexwmdcampus.com. Once registered, click on "public catalog" from the left hand menu and select this course from the list.

Information Security Basics (AWR-173-W)

Information Security Basics is designed to teach entry and mid-level IT staff the technological fundamentals of information security for computer systems and networks. The goal of this course is to provide preliminary knowledge of computer security to help in identifying and stopping various cyber threats. Topics covered include:

- Overview and terminology
- General concepts
- Transmission Control Protocol (TCP)/internet protocol networking
- Network security
- Operating systems and security
- Cryptography

Upon completion of the course, participants may request a certificate of completion provided by DHS FEMA.

To register, go to: www.teexwmdcampus.com. Once registered, click on "public catalog" from the left hand menu and select this course from the list.

Information Security for Everyone (AWR-175-W)

Information Security for Everyone is an entry-level course designed to teach the principles and practices that all computer users need to keep themselves safe, both at work and at home. By presenting best practices along with a small amount of theory, participants will learn both what to do to protect their computer and information, as well as why such steps are necessary. Topics covered include:

- Securing both clean and corrupted systems
- Protecting personal data
- Securing simple computer networks
- Using the internet safely

Upon completion of the course, participants may request a certificate of completion provided by DHS FEMA.

To register, go to: www.teexwmdcampus.com. Once registered, click on "public catalog" from the left hand menu and select this course from the list.

Cybersecurity – Control Systems

Web-Based Format

Cybersecurity for Control Systems Engineers & Operators (CSSP)

Cybersecurity for Control Systems Engineers & Operators is a Web-based training package consisting of five lessons covering threats, risks, cyber attacks, risk assessments, and mitigations for control systems. It can be completed in less than an hour. This course has been approved for North American Electric Reliability Corporation (NERC) continuing education credits.

Online at: http://www.us-cert.gov/control_systems/cstraining.html
Select this course and follow the instructions provided.

OPSEC for Control Systems (CSSP)

Operations Security (OPSEC) for Control Systems is a Web-based training package consisting of seven lessons covering the definition of OPSEC, the five-step OPSEC process, common information-collection techniques, information protection, physical protection, appropriate and inappropriate use in the control system environment, and a summary. It can be completed in less than an hour. This course has been approved for NERC continuing education credits. OPSEC for Control Systems won the 2007 Interagency OPSEC Support Staff National Award for Multimedia Achievement.

Online at: http://www.us-cert.gov/control_systems/cstraining.html
Select this course and follow the instructions provided.

Instructor Led Format – Introductory Level

Introduction to Control Systems Cybersecurity - 101 (CSSP)

The purpose of this course is to introduce students to the basics of industrial control systems security. This includes a comparative analysis of IT and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain.

This 1 day (8 hour) course is split into four sessions: (1) Cybersecurity Landscape: Understanding the Risks, (2) Industrial Control Systems Applications, (3) Current State of Cybersecurity in Industrial Control Systems, and (4) Practical Applications of Cybersecurity.

To request this free, one-day training at your event or venue, e-mail cssp_training@hq.dhs.gov. To determine if this course is being offered at a scheduled event, view the current schedule at http://www.us-cert.gov/control_systems/cscalendar.html.

Industrial Control Systems Security for Management - 111 (CSSP)

This 1 to 2 hour course offers management the necessary background and basic understanding of the current ICS cyber security landscape. This includes an overview of the elements of the risk equation and how it applies to cyber security of an ICS, with an emphasis on threat and its components. The course is designed to introduce the managers to actual threats and vulnerability along with tools they can use to help mitigate the cyber security risk to their ICS.

To request this free training at your event or venue, e-mail cssp_training@hq.dhs.gov. To determine if this course is being offered at a scheduled event, view the current schedule at http://www.us-cert.gov/control_systems/cscalendar.html.

Instructor Led Format – Intermediate Level

Intermediate Cybersecurity for Industrial Control Systems – 201 (CSSP)

This course provides technical instruction on the protection of industrial control systems using offensive and defensive methods. Students will understand how cyber attacks could be launched, why they work, and mitigation strategies to increase the cybersecurity posture of their control system. In addition, this lecture only course acts as a prerequisite for the next course, Intermediate Control System Security-Part 2, which offers hands-on application of the concepts presented.

This course is split into four sessions: (1) Current Security in ICS, (2) Strategies Used Against ICS, (3) Defending the ICS, and (4) Preparation and Further Reading for Part 2.

To request this free, one-day training at your event or venue, e-mail cssp_training@hq.dhs.gov. To determine if this course is being offered at a scheduled event, view the current schedule at http://www.us-cert.gov/control_systems/cscalendar.html.

Hands-on Format – Intermediate Technical Level

Intermediate Cybersecurity for Industrial Control Systems - 202 (CSSP)

This hands-on course is structured to help students understand exactly how attacks against process control systems could be launched and why they work and to provide mitigation strategies to increase the cybersecurity posture of their control systems networks.

This course provides a brief review of industrial control systems security. This includes a comparative analysis of IT and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain. Because this course is hands-on, students will get a deeper understanding of how the various tools work. Accompanying this course is a sample process control network that demonstrates exploits used for unauthorized control of the equipment and mitigation solutions. This network is also used during the course for the many hands-on exercises that will help the students develop control systems cybersecurity skills they can apply when they return to their jobs.

This course is split into six sessions: (1) Supervisory Control and Data Acquisition (SCADA) and control system overview, (2) Risk to Industrial Control Systems, (3) Exploit demonstration, (4) Basic Control Security Considerations, (5) Network: Security, Identification, and Remediation, and (6) Network: Defense, Detection, and Analysis. The goal of the training is to give you an understanding of some key issues in cybersecurity related to industrial control systems. Additionally, it will provide you with hands-on training applying the information learned

To request this free, one-day training at your event or venue, email cssp_training@hq.dhs.gov. To determine if this course is being offered at a scheduled event, view the current schedule at http://www.us-cert.gov/control_systems/cscalendar.html.

Hands-on Format – Advanced Technical Level

ICS Advanced Cybersecurity - 301 (CSSP)

This event will provide intensive hands-on training on protecting and securing industrial control systems from cyber attacks, including a Red Team/Blue Team exercise that will be conducted within an actual control systems environment. This exercise provides an opportunity to network and collaborate with other colleagues involved in operating and protecting control systems networks.

This event includes 5 days of intensive cybersecurity for industrial control systems training, and a Red Team / Blue Team exercise:

- Day 1 — Welcome, overview of the DHS Control Systems Security Program, a brief review of cybersecurity for Industrial Control Systems, a demonstration showing how a control system can be attacked from the internet, and hands-on classroom training on Network Discovery techniques and practices.
- Day 2 — Hands-on classroom training on Network Discovery, using Metasploit, and separating into Red and Blue Teams.
- Day 3 — Hands-on classroom training on Network Exploitation, Network Defense techniques and practices, and Red and Blue Team strategy meetings.
- Day 4 — A 12-hour exercise where participants are either attacking (Red Team) or defending (Blue Team). The Blue Team is tasked with providing the cyber defense for a corporate environment, and with maintaining operations to a batch mixing plant, and an electrical distribution SCADA system.
- Day 5 — Red Team/Blue Team exercise lessons learned and round-table discussion.

Prerequisites: Each attendee should have practical knowledge with ICS networks, software, and components, have basic coding skills, and a fairly deep understanding of IT network details, such as the difference between UDP & TCP protocols, and MAC & IP addresses. **Every student attending this course should bring a laptop computer** (with a DVD drive) that they have "administrator" privileges for, allowing them to configure and load software.

This free training course is only available at the Control Systems Analysis Center in Idaho Falls, Idaho. For more information, email cssp_training@hqdhs.gov. To view the current schedule for this course, go to http://www.us-cert.gov/control_systems/cscalendar.html.

LIST OF ACRONYMS

AWR	Awareness
CFR	Code of Federal Regulations
CIKR	Critical Infrastructure and Key Resources
CS&C	Cyber Security & Communications
CSSP	Control Systems Security Program
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
DOT	U.S. Department of Transportation
EMI	Emergency Management Institute
EMS	Emergency Medical Services
EOTA	Emergency Operations Training Academy
FEMA	Federal Emergency Management Agency
FMCSA	Federal Motor Carrier Safety Administration
GCC	Government Coordinating Council
HSEEP	Homeland Security Exercise and Evaluation Program
HSPD	Homeland Security Presidential Directive
ICS	Industrial Control Systems
IED	Improvised Explosive Device
IP	Office of Infrastructure Protection
IS/ISP	Independent Study / Independent Study Program
IT	Information Technology
MAC	Message Authentication Code
MARSEC	Maritime Security
MGT	Management
NCSD	National Cyber Security Division
NDPC	National Domestic Preparedness Consortium
NERC	North American Electric Reliability Corporation
NFA	National Fire Academy
NFPA	National Fire Protection Association
NGO	Non-Governmental Organization
NPPD	National Protection and Programs Directorate
NRF	National Response Framework
NSEC	National Standard Exercise Curriculum
NTED	National Training and Education Division
OBP	Office for Bombing Prevention
OPSEC	Operations Security

PER	Performance
PSA	Protective Security Advisor
RDPC	Rural Domestic Preparedness Consortium
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SSA	Sector-Specific Agency
SSI	Security Sensitive Information
TCP	Transmission Control Protocol
TEEX	Texas Engineering Extension Service
TIC	Toxic Industrial Chemicals
TIH	Toxic Inhalation Hazard
TSA	Transportation Security Administration
TSNM	Transportation Sector Network Management
TWIC	Transportation Worker Identification Credential
UDP	User Datagram Protocol
VBIED	Vehicle-Borne Improvised Explosive Device
WMD	Weapons of Mass Destruction

Courses
Alphabetized by Category

Category	Course Title	Course Number	Sponsor	Page
Business Planning	Business Continuity and Emergency Management	MGT-381	RDPC	18
	Business Information Continuity	AWR-176-W	TEEX	18
	Protecting Your Home Or Small Business From Disaster	IS-394.A	FEMA Independent Study	19
Cybersecurity - Control Systems	Cybersecurity for Control Systems Engineers & Operators		CSSP	21
	ICS Advanced Cybersecurity - 301		CSSP	23
	ICS Security for Management -111		CSSP	21
	Intermediate Cybersecurity for Industrial Control Systems – 201 (Lecture only)		CSSP	22
	Intermediate Cybersecurity for Industrial Control Systems – 202 (with lab/exercise)		CSSP	22
	Introduction to Control Systems Cybersecurity - 101		CSSP	21
	OPSEC for Control Systems		CSSP	21
Cybersecurity - Information Security	Cyber Incident Analysis and Report	AWR-169-W	TEEX	19
	Information Security Basics	AWR-173-W	TEEX	20
	Information Security for Everyone	AWR-175-W	TEEX	20
Emergency Response	Active Shooter, What You Can Do	IS-907	FEMA Independent Study	17
	Are You Ready? An In-Depth Guide to Citizen Preparedness	IS-22	FEMA Independent Study	17
	Chemical Facility Security: Best Practices Guide for an Active Shooter Incident		Chemical SSA	17
	Emergency Response: Strengthening Cooperative Efforts Among Public Safety and Private Sector Entities	PER-280	RDPC	17
	Get Ready: Prepare, Plan, and Stay Informed		DHS	18
Exercises	An Introduction to Exercises	IS-120.A	FEMA Independent Study	14
	Active Shooter & Workplace Violence Tabletop Exercise and Resources		Chemical SSA	14
	Emergency Planning Exercises for Your Organization		FEMA Private Sector Office	15
	Exercise Evaluation and Improvement Planning	IS-130	FEMA Independent Study	15
	Infrastructure Protection Sector-Specific Tabletop Exercise Program (IP-SSTEP) Chemical Sector Tabletop Exercise (TTX)		Chemical SSA	15
	Major Earthquake Tabletop Exercise		Chemical SSA	16
	Security Seminar & Exercise Series with Chemical Industry Stakeholders		Chemical SSA	16
First Responders	Emergency Response to Terrorism: Self-Study	Q 534	NFA	13

	Rail Car Incident Response	AWR-147	RDPC	14
	WMD/Terrorism Awareness for Emergency Responders	AWR-160-W	TEEX	14
Hazard Mitigation	Introduction to Hazard Mitigation	IS-393.A	FEMA Independent Study	16
Hazardous Materials	An Introduction to Hazardous Materials	IS-5.A	FEMA Independent Study	13
National Incident Management	National Incident Management System, An Introduction	IS-700.A	FEMA Independent Study	7
National Response Framework	National Response Framework, An Introduction	IS-800.B	FEMA Independent Study	7
Security Awareness	Bombing Prevention Workshop		OBP	9
	Chemical Sector Security Awareness Guide: A Guide for Owners, Operators, and Chemical Supply-Chain Professionals		Chemical SSA	8
	Hazmat Motor Carrier Security Self-Assessment Training Program		TSA	9
	IED Awareness/Bomb Threat Management		OBP	9
	IED Search Procedures		OBP	9
	IED Recognition and Detection for Railroad Industry Employees		TSA	10
	Pipeline Security Awareness for the Pipeline Industry Employee		TSA	10
	Port and Vessel Security for Public Safety and Maritime Personnel	AWR-144	RDPC	10
	Private Sector Counterterrorism Awareness Workshop		OBP	10
	Protective Measures Course		OBP	11
	Soft Target Awareness Course		OBP	11
	Surveillance Detection Awareness Discussion Resource Kit		Chemical SSA	8
	Surveillance Detection Training for Commercial Infrastructure Operators and Security Staff		OBP	11
	Vehicle Bomb Search Methods	CIP 110 DC	DOE EOTA	11
	Web-Based Chemical Sector Security Awareness Training		Chemical SSA	8
	Workplace Security Awareness	IS-906	FEMA Independent Study	12
Terrorist Acts/ WMDs	Terrorism and WMD Awareness in the Workplace	AWR-187-W	RDPC	12
	Weapons of Mass Destruction (WMD): General Education	CIP 300 DC	DOE EOTA	12