Facility Security Officer

Model Course CGAA 13-01

Prepared by

U.S. DEPARTMENT OF TRANSPORTATION
MARITIME ADMINISTRATION
UNITED STATES MERCHANT MARINE ACADEMY

for

25 February 2013

DRAFT

Contents

Introduction

This Facility Security Officer (FSO) model course was developed in partial fulfilment of the requirements of the Coast Guard Authorization Act of 2010 (CGAA 2010) (Public Law 111–281). Section 821 of the Act calls for the Secretary of the Department of Homeland Security to establish comprehensive FSO training requirements designed to provide full security training that leads to certification of such officers.

This model course was prepared by the U.S. Merchant Marine Academy for the U.S. Coast Guard in close cooperation with Subject Matter Experts from the regulated facility, maritime training, port authority, and other communities. Their comments and suggestions have helped to ensure that the model course is consistent with applicable industry and government standards and practices, and that the training will maximize security while minimizing negative impacts on port and supply chain productivity. The course has been further refined through input received via a formal public comment process. The assistance of the Subject Matter Experts and the insights provided by other industry contributors are gratefully acknowledged.

The course is intended as specific guidance upon which training providers can base instruction in facility security matters. It is the result of a careful effort to ensure that the requirements of relevant domestic legislation, international conventions, and pertinent guidance are addressed through performance-based standards of competence and learning objectives. It addresses the core knowledge, understanding, and proficiency that must be possessed by FSOs in all U.S. facilities regulated under 33 CFR Part 105. The course is structured so that FSOs working in specialized facilities complete an additional module that focuses on the needs and regulatory requirements associated with that industry sector.

The present course builds on the model curriculum originally developed by the U.S. Maritime Administration (MARAD) in fulfilment of its charge under the Maritime Transportation Security Act of 2002 (MTSA) and work undertaken by MARAD for the International Maritime Organization (IMO). Section 109 of MTSA required the Secretary of Transportation to develop standards and curricula to allow for the certification of maritime security professionals. This responsibility was delegated by the Secretary to MARAD and subsequently assigned to the U.S. Merchant Marine Academy for execution.

Through a cooperative effort with industry and other government agencies, the Academy created six model courses in response to the training needs identified by the Congress and articulated in MTSA. In 2003, the MTSA project led to the creation by the Academy, in a joint effort with the Government of India, of three model maritime security courses for the IMO. In 2011, the Academy developed five additional IMO model courses for vessel and facility personnel.

This model course will serve as the reference for course approval and certification that will be required under U.S. Coast Guard regulation. Previously, IMO Model Course 3.21 (Port Facility Security Officer) was the standard for MARAD approval of FSO training courses.

The Maritime Administration and the U.S. Merchant Marine Academy are proud to have been of service to the Coast Guard, the industry, and the Nation in this effort to enhance port and maritime security.

Part A: Course Framework

Scope

This model course is intended to provide the knowledge required for personnel who are assigned responsibilities as Facility Security Officer (FSO) and those who are designated as Alternate FSO to perform their duties in accordance with the requirements of the Coast Guard Authorization Act of 2010, the Maritime Transportation Security Act of 2002 (MTSA), Chapter XI-2 of SOLAS 74 as amended, the International Ship and Port Facility Security (ISPS) Code, U.S. Coast Guard regulations contained in 33 CFR Subchapter H, and other applicable requirements.

Objective

Those who successfully complete this course must be able to successfully undertake the duties and responsibilities of a designated Facility Security Officer in a facility regulated under 33 CFR Part 105, which include:

1. Ensuring that the Facility Security Assessment (FSA) is conducted;
2. Ensuring the development and implementation of a Facility Security Plan (FSP);
3. Ensuring that an annual audit is conducted, and if necessary that the FSA and FSP are updated;
4. Ensuring that the FSP is exercised per 33 CFR §105.220;
5. Ensuring that regular security inspections of the facility are conducted;
6. Ensuring the security awareness and vigilance of facility personnel;
7. Ensuring adequate training of personnel performing facility security duties;
8. Ensuring that occurrences that threaten the security of the facility are recorded and reported to the owner or operator;
9. Ensuring the maintenance of records required by 33 CFR Part 105;
10. Ensuring the preparation and the submission of any reports required by 33 CFR Part 105;
11. Ensuring the execution of any required Declarations of Security (DOS) with Masters, Vessel Security Officers (VSOs), or their designated representatives;
12. Ensuring the coordination of security services in accordance with the approved FSP;
13. Ensuring that security equipment is properly operated, tested, calibrated, and maintained;
14. Ensuring the recording and reporting of attainment changes in Maritime Security (MARSEC) levels to the owner or operator and the cognizant Captain of the Port (COTP);

15. When requested, ensuring that the VSOs receive assistance in confirming the identity of visitors and service providers seeking to board the vessel through the facility;

16. Ensuring notification, as soon as possible, to law enforcement personnel and other emergency responders to permit a timely response to any transportation security incident;

17. Ensuring that the FSP is submitted to the cognizant COTP for approval, as well as any plans to change the facility or facility infrastructure prior to amending the FSP;

18. Ensuring that all facility personnel are briefed of changes in security conditions at the facility;

19. Ensuring that the TWIC program is being properly implemented; and

20. Ensuring that the FSP provides a system for seamen assigned to a vessel at a port facility, pilots, and representatives of seamen's welfare and labor organizations to board and depart the vessel through the facility in a timely manner at no cost to the individual as required under Section 811 of the Coast Guard Authorization Act of 2010.

Entry standards

Trainees must be 18 years of age or older and able to speak and understand the English language as would be relevant to the duties of an FSO. Facility owners or operators sending candidates for training are responsible for verifying that these conditions are met before referring candidates for training.

In addition, facility owners and operators, facility managers, and others in the facility organization may take this training to enhance their understanding of security requirements affecting the facility. Certain government and law enforcement personnel with a connection to facility security may also benefit from enrolling in the FSO course. Finally, facility owners and operators may wish to provide this training to facility personnel with security duties to promote greater professional competence of these employees in security matters.

Course completion certificate

A certificate shall be issued to those who have successfully completed this course indicating that the holder has completed training as "Facility Security Officer" through an approved course that is consistent with the content of this model course.

Course delivery

The objectives of this course shall be achieved through multiple delivery methods, which may include approved blends of classroom instruction, eLearning, simulation, exercises, videos, etc., noting the critical importance of hands-on exercises and demonstration of competence in the delivery and assessment of comprehensive and effective training.

If the course is to be delivered via eLearning mechanisms, this must be accomplished through synchronous instructor-led or blended approaches that combine face-to-face and online training. There is no topic within the FSO or FSO refresher course that is unsuitable for delivery via eLearning if eLearning is restricted to synchronous instructor-led or blended learning

methodologies. Stand-alone Computer-Based Training (CBT) does not allow the kind of interaction required for effective instruction in the content of this course and for this reason is not an appropriate mechanism for delivery of initial FSO and FSO refresher training.

Course duration

The time allotted for delivery of each topic in this course will vary depending on the composition of a given class, the background and experience of trainees, the skill of the instructor(s), and other factors. Considering this variability, time specifications for individual modules of the course are not given. The total time that will be required to deliver the core course exclusive of any additional modules that may be required is not less than 22 hours.

Course intake limitations

The maximum number of trainees should not exceed 20 where one qualified instructor leads the course and 30 in cases where two qualified instructors conduct the training.

Instructor Qualifications

The instructor(s) facilitating the course shall have had training and/or acceptable equivalent practical experience in the subject matter of this course, including knowledge of facility operations; maritime security matters; and the requirements of the Coast Guard Authorization Act of 2010, the Maritime Transportation Security Act of 2002 (MTSA), Chapter XI-2 of SOLAS 74 as amended, the International Ship and Port Facility Security (ISPS) Code, U.S. Coast Guard regulations contained in 33 CFR Subchapter H, and other applicable requirements.

Instructors shall be certified FSOs, having successfully completed FSO training based on this model course or training accepted by the Coast Guard as being equivalent thereto. Instructors who have previously completed MARAD-approved FSO training are considered qualified in this regard.

It is recommended that instructors have appropriate training in or be familiar with instructional techniques and training methods.

Teaching facilities and equipment

Conventional lectures can be delivered in a properly-appointed classroom or similar meeting room with a blackboard, whiteboard, or electronic equivalent for information display. Appropriate computer equipment and displays must be available if simulations or interactive computer-based training are employed. Audio-visual aids, such as CD/DVD players, televisions, etc., are helpful in providing variety in the delivery of course material.

The use of charts, maps, facility mock-ups, etc., for certain segments of the course may enhance the overall effectiveness of this training.

Teaching aids

The following teaching aids may be useful in the delivery of the course:

1. Photographs, models, or other representations of facilities, vehicles, dangerous devices, etc., to illustrate operational elements and security vulnerabilities.
2. CDs/DVDs
3. Distance learning packages
4. PowerPoint presentations
5. Training workbooks
6. Training reference documents

Training references

The following references may be useful to instructors in delivering the course material. They may be provided to trainees as resources as appropriate. It should be noted that these references include government regulations and guidance that are in effect at the time of course publication, but which are subject to change. Course providers should ensure that their instruction is based on the most current laws, regulations, and official guidance.

Christopher, K. (2009). *Port Security Management.* Boca Raton: Auerbach.

Coast Guard, Department of Homeland Security. *33 CFR (Navigation and Navigable Waters), Chapter I, Subchapter H—Maritime Security, Parts 101, 102, 103, 104, 105, 106, and 108.*

Coast Guard, Department of Homeland Security. *33 CFR (Navigation and Navigable Waters), Chapter I, Subchapter L—Waterfront Facilities, Part 126.*

Coast Guard, Department of Homeland Security. *46 CFR (Shipping), Part 4—Marine Casualties and Investigations.*

Coast Guard. *Risk Based Decision Making: Risk-based Decision Making Guidelines.* http://www.uscg.mil/hq/cg5/cg5211/E-Guidelines.asp.

Commandant, United States Coast Guard. (2002, 29 March). "Security for Passenger Vessels and Passenger Terminals." *Navigation and Vessel Inspection Circular (NVIC) No. 04-02.*

Commandant, United States Coast Guard. (2003, 15 December). "Implementation Guidance for the Maritime Security Regulations Mandated by the Maritime Transportation Security Act of 2002 for Outer Continental Shelf Facilities." *Navigation and Vessel Inspection Circular (NVIC) No. 05-03.*

Commandant, United States Coast Guard. (2004, 20 August). "Guidelines for Handling of Sensitive Security Information (SSI)." *Navigation and Vessel Inspection Circular (NVIC) No. 10-04.*

Commandant, United States Coast Guard. (2004, 27 May). "Voluntary Screening Guidance for Owners or Operators Regulated under Parts 104, 105, and 106 of Subchapter H of Title 33, Code of Federal Regulations." *Navigation and Vessel Inspection Circular (NVIC) No. 06-04.*

Commandant, United States Coast Guard. (2004, 6 August). "Recommended Security Guidelines for Facilities." *Navigation and Vessel Inspection Circular (NVIC) No. 11-02, Change 1.*

Commandant, United States Coast Guard. (2004, 6 August). "Security Guidelines for Vessels." *Navigation and Vessel Inspection Circular (NVIC) No. 10-02, Change 1.*

Commandant, United States Coast Guard. (2007, 2 July). "Guidance for the Implementation of the Transportation Worker Identification Credential (TWIC) Program in the Maritime Sector." *Navigation and Vessel Inspection Circular (NVIC) No. 03-07*.

Commandant, United States Coast Guard. (2008, 29 April). "Guidelines for Development of Area Maritime Security Committees and Area Maritime Security Plans Required for U.S. Ports." *Navigation and Vessel Inspection Circular (NVIC) No. 09-02, Change 3.*

Commandant, United States Coast Guard. (2009, 28 February). "Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 (MTSA) for Facilities." *Navigation and Vessel Inspection Circular (NVIC) No. 03-03, Change 2.*

Department of Health and Human Services. *21 CFR (Food and Drugs), Chapter 1, Subchapter A--General, Parts 1 and 11.*

Department of Homeland Security. *6 CFR (Domestic Security), Chapter I, Parts 25, 27, and 29.*

Department of Homeland Security. (2010). DHS Risk Lexicon—2010 Edition. http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

Department of Homeland Security. Federal Emergency Management Agency. Incident Command System. http://www.fema.gov/incident-command-system

Department of Homeland Security. Federal Emergency Management Agency. NIMS Overview Presentation. http://www.fema.gov/library/viewRecord.do?id=6449

Department of Transportation. Pipeline and Hazardous Materials Safety Administration. *49 CFR (Transportation), Subtitle B—Other Regulations Relating to Transportation, Chapter 1.*

Department of Transportation. Volpe National Transportation Systems Center. (1999). *Intermodal Cargo Transportation: Industry Best Security Practice*s. Cambridge: Volpe Center.

Fernandez, L., & Merzer, M. (2003). *Jane's Crisis Communications Handbook*, (1st ed.). Alexandria: Jane's Information Group.

FIA International Research, Ltd. (2001). *Contraband, Organized Crime and the Threat to the Transportation and Supply Chain Functio*n. FIA International.

Government Accountability Office. (2007). *The SAFE Port Act and Efforts to Secure Our Nation's Seaports.* (GAO-08-86T).

Interagency Commission on Crime and Security in U.S. Seaports. (2000). *Report of the Interagency Commission on Crime and Security in U.S. Seaport*s. Washington, D.C.

International Labour Organization. *Seafarers' Identity Documents Convention (Revised), 2003*. (No. 185).

International Maritime Organization. (2003). *International Ship & Port Facility Security (ISPS) Code, 2003 and December 2002 Amendments to SOLAS*. London: IMO. (IMO-I116E).

International Maritime Organization. (2004). *MSC/Circ.1112--Shore Leave and Access to Ships under the ISPS Code.*

International Maritime Organization. (2006). *MSC.1/Circ.1188—Guidelines on Training and Certification for Port Facility Security Officers.*

International Maritime Organization. (2006). *MSC.1/Circ.1194-- Effective Implementation of SOLAS Chapter XI-2 and the ISPS Code.*

International Maritime Organization. (2009). *International Convention for the Safety of Life at Sea (SOLAS), 1974 (Consolidated edition)*. London: IMO. (IMO-IE110E).

International Maritime Organization. (2010). *MSC.1/Circ.1341—Guidelines on Security-related Training and Familiarization for Port Facility Personnel.*

McNicholas, M. (2007). *Maritime Security: An Introduction.* Burlington: Butterworth-Heinemann.

Nationwide SAR Initiative (NSI). Online SAR Training for Law Enforcement and Hometown Security Partners http://nsi.ncirc.gov/training_online.aspx.

Sidell, F. R., et al. (2002). *Jane's Chem-Bio Handbook*. (2nd ed.). Alexandria: Jane's Information Group.

Sullivan, J. P., et al. (2002). *Jane's Unconventional Weapons Response Handbook.* (1st ed.). Alexandria: Jane's Information Group.

Transportation Security Administration, Department of Homeland Security. *49 CFR (Transportation), Subtitle B—Other Regulations Relating to Transportation, Chapter Xii, Subchapter B—Security Rules for All Modes of Transportation, Part 1520.*

Transportation Security Administration, Department of Homeland Security. *49 CFR (Transportation), Subtitle B—Other Regulations Relating to Transportation, Chapter Xii, Subchapter D—Maritime and Land Transportation Security.*

TWIC/MTSA Policy Advisory Council. (2008, September 30). "Policy: TWIC Requirements and Rail Access into Secure Areas" (PAC 05-08).

United States Congress. (2002, 25 November). *Maritime Transportation Security Act of 2002 (P.L. 107-295)*.

United States Congress. (2006, 13 October). *Security and Accountability for Every Port Act Of 2006 (P.L. 109-347).*

United States Congress. (2010, 15 October). *Coast Guard Authorization Act of 2010 (P.L. 111-281)*.

Part B: Course Outline

The following outline delineates the topics that should be covered in the FSO course. Training providers and instructors may wish to reorganize the order in which the material is to be presented to reflect the needs of a particular audience and/or the preferences and teaching methods of the instructor(s) in charge of the course.

Subject Area
1. Introduction
1.1. Course overview
1.2. Criminal activity in the maritime environment
1.3. Current security threats
2. Maritime Security Regulation and Policy
2.1. Definitions and acronyms
2.2. International conventions and codes
2.3. U.S. legislation and regulations
2.4. U.S. Coast Guard directives, bulletins, and guidance
2.5. Area Maritime Security
2.6. Alternatives and equivalents
3. Facility Security Organization and Responsibilities
3.1. Federal government agencies
3.2. State government agencies
3.3. Local government agencies
3.4. Jurisdictional issues
3.5. Owner or operator
3.6. Facility Security Officer
3.7. Facility personnel with security duties
3.8. All other facility personnel
3.9. Vessel security organization

4. Facility Security Measures

4.1. Physical security

4.2. Access control

4.3. Newly-hired employees

4.4. Restricted Areas

4.5. Handling cargo

4.6. Delivery of vessel stores and bunkers

4.7. Monitoring

5. Security Technology and Cybersecurity

5.1. Types and functions of security equipment and systems

5.2. Operational limitations of security equipment and systems

5.3. Testing, calibration, and maintenance of security equipment and systems

5.4. Evaluation and selection of facility security technology

5.5. Information assurance and cybersecurity

6. Threat Recognition and Detection

6.1. Recognition and detection of dangerous substances and devices

6.2. Recognition of persons posing potential security risks

6.3. Physical screening and non-intrusive inspections

6.4. Conducting security sweeps and searches

6.5. Techniques used to circumvent security measures

6.6. Internal conspiracies/sabotage

7. MARSEC Levels and Incident Response

7.1. MARSEC level coordination and implementation

7.2. The Declaration of Security (DoS)

7.3. Security incident responsibilities

7.4. Security-related communications

7.5. Reporting security incidents

7.6. Interfacing with first responders

7.7. Evacuation of the facility

7.8. Emergency Operations Plan (EOP)

8. Security Training, Drills, and Exercises

8.1. Training requirements

8.2. Instructional techniques

8.3. Requirements for security drills and exercises

8.4. Assessment of security drills and exercises

9. Security Administration

9.1. Handling Sensitive Security Information (SSI)

9.2. Documentation and record retention

9.3. Facility security force management (as appropriate)

10. Facility Security Assessment (FSA)

10.1. Risk assessment methods

10.2. Facility Security Assessment requirements

10.3. Background

10.4. On-scene security surveys

10.5. Analysis and recommendations

10.6. FSA Report

10.7. Submission requirements

11. Facility Security Plan (FSP)

11.1. Facility Security Plan requirements

11.2. Format and content of the FSP

11.3. Submission and approval of the FSP

11.4. Amendment and audit of the FSP

11.5. Use of Form CG-6025 or subsequent version

11.6. Compliance inspections

12. Trainee Assessment
12.1. Assessment of knowledge, understanding, proficiency, and skill
Minimum Core Course Duration: 22 hours

Additional Module: Container Facilities (*See Sample Module in Appendix A*)
Additional Module: Certain Dangerous Cargo (CDC) Facilities
Additional Module: Passenger and Ferry Facilities
Additional Module: Cruise Ship Facilities
Additional Module: Barge Fleeting Facilities
Additional Module: Outer Continental Shelf (OCS) Facilities

Part C: Detailed Teaching Syllabus

Competences

Those who successfully complete this course will have demonstrated knowledge, understanding, and proficiency in the following competences:

1. Developing, maintaining, and supervising the implementation of a Facility Security Plan;

2. Assessing security threats, vulnerabilities, and risk;

3. Undertaking regular inspections of the facility to ensure that appropriate security measures are implemented and maintained;

4. Ensuring that security equipment and systems are properly operated, tested, and calibrated;

5. Encouraging security awareness and vigilance; and

6. Ensuring compliance with the TWIC program requirements.

Learning Objectives

The detailed teaching syllabus has been written in learning objective format in which the objective describes the knowledge, understanding, and proficiency that must be demonstrated by a trainee in order to successfully complete the course. Objectives are understood to be prefixed by the words, "Upon completion of this course, the expected learning outcome is that the student will be able to _____."

1. Introduction

1.1. Course overview

.1 describe the organization and focus of the course

.2 list the competences that will be achieved through completion of the course

1.2. Criminal activity in the maritime environment

.1 describe representative historical incidents of maritime crime

.2 summarize maritime crime incident statistics

.3 discuss the known and suspected motivations for and potential impacts of maritime criminal activity

1.3. Current security threats

.1 distinguish between man-made and natural threats to security

.2 summarize the all-hazards approach to maritime security

.3 identify the current primary threats to maritime security

2. Maritime Security Regulation and Policy

2.1. Definitions and acronyms

.1 define key terms, acronyms, and abbreviations used in maritime security

2.2. International conventions and codes

.1 list the principal international instruments that impact maritime security

.2 describe the significance of the principal international instruments that impact maritime security

2.3. U.S. legislation and regulations

.1 list the principal U.S. laws and rules affecting maritime security

.2 state the focus of the principal U.S. laws and rules affecting maritime security

2.4. U.S. Coast Guard directives, bulletins, and guidance

.1 identify the key types of USCG documents and information releases that update and convey changes in interpretations of maritime security regulation and policy

2.5. Area Maritime Security

.1 discuss the nature and purpose of an Area Maritime Security Committee (AMSC)

2.6. Alternatives and equivalents

.1 describe the nature of alternative security programs and equivalent security measures provided for in maritime security regulations

.2 explain procedures for developing and obtaining approval of alternative security programs and equivalent security measures

3. Facility Security Organization and Responsibilities

3.1. Federal government agencies

.1 list the principal federal government agencies associated with maritime security and their functions

.2 identify strategies for interactions with federal government agencies

3.2. State government agencies

.1 list the principal state government agencies associated with maritime security and their functions

.2 identify strategies for interactions with state government agencies

3.3. Local government agencies

.1 list the principal local government agencies associated with maritime security and their functions

.2 identify strategies for interactions with local government agencies

3.4. Jurisdictional issues

.1 characterize the problem of competing and overlapping regulations and jurisdictions

3.5. Owner or operator

.1 summarize the responsibilities of the owner/operator as defined by maritime security regulations and policy

3.6. Facility Security Officer

.1 state the requirement that a Facility Security Officer be designated for each facility

.2 explain the circumstances in which a person may be designated as the Facility Security Officer for one or more facilities

.3 list the duties and responsibilities of the Facility Security Officer

3.7. Facility personnel with security duties

.1 state that facility personnel other than the FSO may be assigned security duties in support of the Facility Security Plan

3.8. All other facility personnel

.1 describe how other facility personnel can contribute to the enhancement of maritime security

.2 describe how visitors to the facility can contribute to the enhancement of maritime security

3.9. Vessel security organization

.1 note that each vessel has a Vessel Security Officer with shipboard responsibilities that parallel those of the FSO for the facility

.2 note that vessels have personnel with security duties with shipboard responsibilities that parallel those of facility personnel with security duties

.3 describe how other vessel personnel can contribute to the enhancement of maritime security

.4 describe how visitors to the vessel can contribute to the enhancement of maritime security

4. Facility Security Measures

4.1. Physical security

.1 describe the basic elements of physical security

4.2. Access control

.1 summarize the security measures for access control required by regulation

.2 explain the requirements of the TWIC program

.3 summarize the security measures required for secure areas

.4 note the varying requirements for access control at different MARSEC levels

.5 explain the requirements for TWIC escorting

.6 identify the characteristics of public access areas

.7 describe requirements for facilitating mariner shore leave, providing visitor access, and handling the issue of detained crewmembers

.8 note the access control issues unique to rail operations

4.3. Newly-hired employees

.1 summarize the security measures required for newly-hired employees

4.4. Restricted areas

.1 summarize the security measures required for restricted areas

4.5. Handling cargo

.1 summarize the security measures required for handling cargo

4.6. Delivery of vessel stores and bunkers

.1 summarize the security measures required for delivery of stores and bunkers

4.7. Monitoring

.1 summarize the requirements for continuous monitoring of the facility, its approaches, and vessels at the facility in accordance with the approved FSP

.2 note the varying requirements for monitoring at different MARSEC levels

5. Security Technology and Cybersecurity

5.1. Types and functions of security equipment and systems

.1 list the principal types of security equipment and systems that are currently used in the facility environment

.2 describe the functions of security equipment and systems that are currently used in the facility environment

5.2. Operational limitations of security equipment and systems

.1 explain the limitations of security equipment and systems that are currently used in the facility environment

5.3. Testing, calibration, and maintenance of security equipment and systems

.1 summarize the importance of testing and calibration of facility security equipment

.2 explain the importance of security equipment and system maintenance

5.4. Evaluation and selection of facility security technology

.1 discuss the importance of identifying facility technology needs

.2 describe factors to consider in procuring security equipment

5.5. Information assurance and cybersecurity

.1 summarize the current use of information technology in facility operations

.2 explain common threats to security in the facility environment

.3 discuss strategies for enhancing cybersecurity in facility operations

6. Threat Recognition and Detection

6.1. Recognition and detection of dangerous substances and devices

.1 describe the various types of dangerous substances and devices, their appearance, and their potential effects

.2 state the appropriate action to be taken when dangerous substances and devices are discovered

6.2. Recognition of persons posing potential security risks

.1 describe the general characteristics and behavioral patterns of persons who are likely to threaten security

6.3. Physical screening and non-intrusive inspections

.1 demonstrate how to carry out effective physical screening of persons, personal effects, baggage, cargo, and vessel stores

.2 note the need for coordination with ships' agents on aspects of screening

.1 describe the proper use of metal detectors, X-ray machines, and other devices that may be used in non-intrusive inspections, as appropriate

6.4. Conducting security sweeps and searches

.1 describe methods for conducting security sweeps of the facility

.2 summarize the procedures to be followed for an efficient search

.3 state the various places of concealment in a facility

6.5. Techniques used to circumvent security measures

.1 describe the techniques that may be used to circumvent security measures

6.6. Internal conspiracies/sabotage

.1 discuss the nature of internal conspiracies and their role in circumventing security measures

.2 discuss the threat of sabotage in facility operations

7. MARSEC Levels and Incident Response

7.1. MARSEC level coordination and implementation

.1 state the meaning of each MARSEC level

.2 note who is authorized to change the MARSEC level at a facility and aboard a vessel

.3 summarize the requirements for coordination and implementation at each MARSEC level change

.4 note the existence of regulatory requirements for additional security measures that must be implemented in specialized facilities at each MARSEC level

.5 state the importance of adhering to established procedures for interfacing with vessels at all MARSEC levels

7.2. The Declaration of Security (DoS)

.1 explain the DoS and its purpose

.2 describe conditions in which a DoS or revised DoS is required

.3 state who is required to complete the DoS

7.3. Security incident responsibilities

.1 summarize the regulatory responsibilities of the FSO and other security personnel in the event of a transportation security incident or breach of security

7.4. Security-related communications

.1 state the critical importance of communications in facility security management

.2 explain the requirement for redundant communications mechanisms and systems

7.5. Reporting security incidents

.1 explain the procedures for reporting suspicious activities, breaches of security, and Transportation Security Incidents to the National Response Center, the COTP, and other authorities as appropriate

7.6. Interfacing with first responders

.1 explain the importance of adhering to established procedures for interfacing with first responders

.2 note the existence of Incident Command System (ICS) protocols

7.7. Evacuation of the facility

.1 discuss procedures for evacuation and partial evacuation of the facility and the shelter-in-place concept as an alternative, if appropriate

7.8. Emergency Operations Plan (EOP)

.1 explain the importance of an Emergency Operations Plan during and after a crisis

8. Security Training, Drills, and Exercises

8.1. Training requirements

.1 identify which facility personnel must receive training

.2 summarize the subjects in which facility personnel must be trained

.3 note the importance of continuing education and training

8.2. Instructional techniques

.1 summarize methods for delivering security training to facility personnel

8.3. Requirements for security drills and exercises

.1 summarize the purposes of drills and exercises

.2 explain the difference between drills and exercises

.3 state the regulatory requirements for conducting drills and exercises

.4 note that security drills may be held in conjunction with safety drills

8.4. Assessment of security drills and exercises

.1 state the purpose of carrying out an assessment at the end of each drill or exercise

.2 explain the importance of identifying and recording best practices and lessons learned at the end of each drill or exercise

.3 state the need for documentation of follow-up and corrective actions taken to address opportunities and deficiencies noted during drills and exercises

9. Security Administration

9.1. Handling Sensitive Security Information (SSI)

.1 state the requirement to protect specifically identified security-related documents from unauthorized access or disclosure

.2 identify facility security documents and information that are designated as SSI

.3 describe required markings, controls, and methods for the protection and handling of SSI

9.2. Documentation and record retention

.1 identify specific security-related records that are required to be maintained by the FSO

.2 state the regulatory recordkeeping and control requirements for retaining SSI and additional security-related documentation

.3 note that facility security documentation must be made available to the USCG on request

9.3. Facility security force management (as appropriate)

.1 describe alternative forms of security force composition and structure

.2 identify key elements of security force operations such as shifts, patrols, equipment, command centers, etc.

.3 explain the importance of systematic recruiting and pre-employment screening in developing an effective security force

.4 state the importance of proper and continuing training in security force operations

.5 note that liability issues may arise in connection with security force operations

10. Facility Security Assessment (FSA)

10.1. Risk assessment methods

.1 note that there are many risk assessment methods in existence

.2 summarize use of the Risk Based Decision Making (RBDM) approach

10.2. Facility Security Assessment requirements

.1 list the required elements of an FSA

.2 state the conditions under which third parties may conduct the FSA

.3 explain the role of third parties in the FSA process

10.3. Background

.1 characterize the background information that must be available when conducting an FSA

10.4. On-scene security surveys

.1 explain the examination and evaluation of facility protective measures, procedures, and operations

10.5. Analysis and recommendations

.1 explain the risk-based analysis of facility background information and the results of the on-scene survey

.2 describe the development of recommendations to establish and prioritize the security measures that should be included in the FSP

10.6. FSA Report

.1 explain the purpose of the FSA report

.2 summarize the preparation of the FSA report and the information that must be included in it

10.7. Submission requirements

.1 describe the requirements for submission of the FSA report and related documents

.2 explain the requirement for review and validation of the FSA report

.3 note the requirement for updating the FSA report

11. Facility Security Plan (FSP)

11.1. Facility Security Plan requirements

.3 explain the purpose of an FSP

.4 summarize the general regulatory requirements concerning an FSP

.5 state that the FSP is considered SSI and that it must be protected accordingly

.6 explain that if the FSP is kept in an electronic format, procedures must be in place to prevent its unauthorized deletion, destruction, or amendment

11.2. Format and content of the FSP

.1 summarize the specific elements that must be addressed in the FSP

.2 explain that the FSP must demonstrate how the requirements of 33 CFR Part 105 Subpart B are being met at the facility

11.3. Submission and approval of the FSP

.1 describe the procedure for submitting the FSP to the USCG COTP

.2 discuss possible responses of the COTP to an FSP submission

11.4. Amendment and audit of the FSP

.1 list the circumstances in which the FSP may be amended

.2 summarize the requirements for audits of the FSP

.3 explain the key ways in which audits are conducted

.4 describe the possible outcomes of an audit

.5 note the critical importance of using professionally qualified auditors

11.5. Use of Form CG-6025 or subsequent version

.1 describe the use of Form CG-6025 to summarize facility security vulnerabilities and information in the FSP concerning their mitigation

11.6. Compliance inspections

.1 describe the two primary types of USCG inspections

.2 explain how to prepare for compliance inspections

.3 list the possible outcomes of compliance inspections

12. Trainee Assessment

12.1. Assessment of knowledge, understanding, proficiency, and skill

.1 Demonstrate mastery of course material through appropriate assessments

Minimum Core Course Duration: <u>22 hours</u>

Part D: Instructor Manual

The instructor manual provides guidance on the material that is to be presented during the Facility Security Officer course. The guidance given indicates the focus of each section and describes the essential material for which an FSO will be required to demonstrate competency. Instructors should work to identify the level of knowledge possessed by trainees at the outset of the course so that presentation of the material can be adapted to suit the background and expertise of students in a given class.

The main course ("core course") identifies the material that constitutes a "common body of knowledge" required for all FSOs. In addition, FSOs working in specific industry segments (e.g. the cruise sector, container terminals, CDC facilities, etc.) will require additional training in certain topics and content. For this purpose, the core refresher course is extended by separate modules that address the requirements of specialized facilities (*see sample Container Facilities module in Appendix A).*

The material has been arranged under the following 12 main headings:

1. Introduction
2. Maritime Security Regulation and Policy
3. Facility Security Organization and Responsibilities
4. Facility Security Measures
5. Security Technology and Cybersecurity
6. Threat Recognition and Detection
7. MARSEC Levels and Incident Response
8. Security Training, Drills, and Exercises
9. Security Administration
10. Facility Security Assessment (FSA)
11. Facility Security Plan (FSP)
12. Trainee Assessment

The detailed teaching syllabus and the instructor manual should be studied carefully and lesson plans or lecture notes should be compiled based upon them in order to ensure that trainees achieve a knowledge level sufficient to enable them to successfully demonstrate the specified competencies. Preparation and planning are the most important criteria in effectively presenting this course. Availability and proper use of course materials and delivery systems are also essential for maximum efficacy in conveying the content to trainees.

Lectures should be supported by practical demonstrations, table-top exercises, team exercises, simulations, and other approaches that allow the trainee to apply and integrate the material taught online and/or in the classroom. When conducted under the guidance of a qualified instructor, these are excellent opportunities for students to pull together the material they have acquired and to use it in "real world" fashion. These approaches also allow the instructor to identify and correct any weaknesses or gaps in the learning process.

Instructors should assemble examples of policies, procedures, and practices that they deem to represent effective practice in facility security management. These examples may relate to virtually any of the topics that have been covered in the course, and should be chosen to provide trainees with clear and positive models of how to approach a particular security

management task or challenge. Discussion of “common practice” examples of such aspects of facility security as equipment selection and deployment, facility security measures, intelligence gathering, facility security assessment, etc., will help course participants to integrate the knowledge they acquire during the course and to apply it in their role as FSOs.

Assessment of competence is discussed in the final section of the course.

Guidance Notes

1. Introduction

1.1 Course overview

The instructor will ordinarily begin the course by introducing him/herself and making a brief statement of the objectives of the course. A review of the course schedule and related administrative matters is appropriate, as is a brief description of the teaching facility and associated equipment (in the case of classroom instruction). Instructors may wish to ask participants to introduce themselves and to summarize their backgrounds. It is also desirable to determine the knowledge and experience possessed by each student to assist in targeting the material most effectively. It may be feasible to accomplish this at the beginning of the course by means of surveys and pre-tests.

It should be explained to students that the primary objective of the course is to enable them to acquire and demonstrate the competences listed at the beginning of Part C of the course.

1.2 Criminal activity in the maritime environment

In this section of the course, the instructor should provide a historical perspective on the types of crime that affect port facilities. Representative examples of such activities as smuggling, terrorism, cargo theft, and others should be provided. Summary statistics on the frequency, trends, and impacts of maritime crimes over time should be given. The motivations underlying the various forms of maritime criminal activity should be summarized. The thrust of this section of the course should be to give trainees a foundation that will allow them to understand the character and significance of current security threats.

1.3 Current security threats

The discussion of current security threats should provide participants with a sense of the importance and urgency involved in the preservation and enhancement of port and maritime security. Trainees should be made to realize that a wide range of man-made and naturally-occurring threats should be reflected in security planning.

Examples of the types of threats to be considered include the following:

- Accidents
- Active shooters
- Armed assailants
- Bomb threats
- Cargo theft
- Chemical releases
- Collateral damage
- Contraband smuggling
- Cyberattack/failure
- Earthquakes
- Explosions
- Fires

- Human trafficking
- Insider threats
- Power failure
- Robbery and armed attacks
- Sabotage
- Stowaways and refugees
- Terrorism
- Weather extremes
- Workplace violence

There are many elements of prevention, preparedness, response, and recovery that are common to transportation incidents, natural disasters, man-made calamities, and terrorist attacks. Given this, and consistent with the systems view that is essential to efficient and effective analysis of security issues and best use of assets, an "all-hazards" approach to maritime security training is emphasized. It should be made clear that there is significant intersection between security and safety in ports, vessels, and facilities.

The integration of safety, security, and commercial considerations in maritime security should be explained to trainees as an objective that will enable facilities to best mitigate, respond, and recover from the effects of hazards of all kinds.

2. Maritime Security Regulation and Policy

2.1 Definitions and acronyms

Students should be made aware that the maritime industry and security operations and regulation associated with it utilize a large number of specialized terms, abbreviations, and acronyms. Examples of terms with which FSOs should be familiar include the following:

- Alternative Security Program (ASP)
- Area Maritime Security Committee (AMSC)
- Area Maritime Security Plan (AMSP)
- Area of Responsibility (AOR)
- Awareness
- Breach of security
- CG-6025
- Captain of the Port (COTP)
- Certain Dangerous Cargo (CDC)
- Coast Guard (USCG)
- Code of Federal Regulations (CFR)
- Customs and Border Protection (CBP)
- Declaration of Security (DoS)
- Department of Homeland Security (DHS)
- Drill
- Escorted Access
- Exercise

- Facility
- Facility Security Assessment (FSA)
- Facility Security Assessment Report (FSA report)
- Facility Security Officer (FSO)
- Facility Security Plan (FSP)
- Federal Bureau of Investigation (FBI)
- Federal Emergency Management Agency (FEMA)
- Federal Maritime Security Coordinator (FMSC)
- Immigration and Customs Enforcement (ICE)
- Incident Command System (ICS)
- Infrastructure
- International Maritime Organization (IMO)
- International Ship and Port Facility Security (ISPS) Code
- International voyage
- Maritime Administration (MARAD)
- Maritime Security (MARSEC) Directive
- Maritime Transportation Security Act of 2002 (MTSA)
- MARSEC Level
- National Incident Management System (NIMS)
- National Terrorism Advisory System (NTAS)
- Navigation and Vessel Inspection Circular (NVIC)
- Non-Intrusive Inspection (NII)
- On-scene survey
- Outer Continental Shelf (OCS)
- Policy Advisory Council (PAC)
- Public access area
- Public access facility
- Radiation Portal Monitor (RPM)
- Restricted area
- Safety of Life at Sea (SOLAS) Convention
- Screening
- Secure area
- Security sweep
- Security system
- Sensitive Security Information (SSI)
- SOLAS vessel
- Suspicious activity
- Transportation Security Administration (TSA)
- Transportation Security Incident (TSI)
- Transportation Worker Identification Credential (TWIC)
- TWIC Secure/Restricted area
- Unescorted access

- Vehicle and Cargo Inspection System (VACIS)
- Vessel Security Assessment (VSA)
- Vessel Security Officer (VSO)
- Vessel Security Plan (VSP)
- Vessel-to-facility interface
- Vessel-to-vessel activity

Instructors should point out to course participants that most of these terms are defined in 33 CFR §101.105.

2.2 International conventions and codes

ISPS Code

The primary objective of this section of the course is to briefly familiarize trainees with the key provisions of the International Maritime Organization (IMO) International Ship and Port Facility Security (ISPS) Code. This topic is important because the ISPS Code is the foundation of U.S. domestic maritime security regulation. Trainees should understand the origins of the ISPS Code, its connection with the International Convention for the Safety of Life at Sea (SOLAS Convention), and the impact of the Code as the principal international instrument governing port and maritime security.

It should be explained that the ISPS Code is a comprehensive set of measures intended to enhance the security of ships and port facilities, and that it was developed in response to the perceived threat to maritime assets worldwide following the terrorist attacks on 9/11. It should be noted that the ISPS Code is implemented through Chapter XI-2 (Special Measures to Enhance Maritime Security) in the SOLAS Convention. Instructors will point out that the Code has two parts, one mandatory and one recommendatory, but that domestic regulations have, for the most part, made the recommended portion of the Code mandatory in the U.S.

According to the IMO:

> …the Code takes the approach that ensuring the security of ships and port facilities is a risk management activity and that, to determine what security measures are appropriate, an assessment of the risks must be made in each particular case. The purpose of the Code is to provide a standardised, consistent framework for evaluating risk, enabling Governments to offset changes in threat with changes in vulnerability for ships and port facilities through determination of appropriate security levels and corresponding security measures.[1]

2.3 U.S. legislation and regulations

Trainees should be familiarized with the key provisions of U.S. legislation and regulations intended to enhance maritime security. Principal among these are the Maritime Transportation Security Act (MTSA) of 2002, the Security and Accountability for Every Port Act (SAFE Port Act) of 2006, the Coast Guard Authorization Act of 2010, and regulations contained in the U.S. Code of Federal Regulations (CFR), particularly 6 CFR, 33 CFR, 21 CFR, 46 CFR, and 49 CFR. The principal aim of this section is to provide an overview of U.S. laws and USCG/DHS regulations pertaining to maritime security.

[1] IMO. ISPS Code. http://www.imo.org/ourwork/security/instruments/pages/ispscode.aspx

MTSA

The "Maritime Transportation Security Act (MTSA) of 2002" (P.L. 107-295) was enacted by the U.S. Congress on November 25, 2002. MTSA amends the Merchant Marine Act of 1936 to "establish a program of greater security for United States seaports, and for other purposes." The Congress, in enacting MTSA, noted the pivotal role of ports in the economy of the United States, the difficulties inherent in attempting to secure the Nation's port and intermodal transportation system, the vulnerabilities of that system to acts of terrorism, and the diverse types of federal crimes that are committed in the port environment.[2]

Some of the key provisions and requirements of MTSA that relate to security are as follows:

- Requirements for port, facility, and vessel security assessments
- Preparation by the Secretary of Transportation of a National Maritime Transportation Security Plan and Area Plans for each U.S. Coast Guard Captain of the Port Zone
- Development of security plans for certain facilities and commercial vessels
- The issuance and use of Transportation Security Cards for personnel whose responsibilities require them to access secure spaces aboard ships
- Establishment of a permanent program of grants to facilitate the enhancement of maritime security
- Assessment by the Secretary of Transportation of the effectiveness of antiterrorism measures at foreign ports
- Establishment of an enhanced system of foreign seafarer identification
- Creation of Maritime Security Advisory Committees at national and area levels
- Establishment of a program to better secure international intermodal transportation systems, to include cargo screening, tracking, physical security, compliance monitoring, and related issues.
- Provision of civil penalties for violation of statutes or regulations
- Development of standards and curricula for maritime security professional training

SAFE Port Act

The Security and Accountability for Every Port Act (SAFE Port Act) of 2006 (P.L. 109-347) added new port and maritime security requirements and amended certain provisions of the MTSA. The SAFE Port Act included provisions that (1) codified the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT), two programs administered by Customs and Border Protection (CBP) to help reduce threats associated with cargo shipped in containers; (2) required interagency operational centers where agencies organize to fit the security needs of the port area at selected ports; (3) set an implementation schedule and fee restrictions for TWIC; (4) required that all containers entering high volume U.S. ports be scanned for radiation sources by December 31, 2007; and (5) required additional data be made available to CBP for targeting cargo containers for inspection.

The SAFE Port Act also established the Domestic Nuclear Detection Office (DNDO) as an agency within the Department of Homeland Security. DNDO is now the primary entity in the

[2] *United States Congress.* (2002, 25 November). *Maritime Transportation Security Act of 2002 (P.L. 107-295)*. Sec. 101: Findings, 116 Stat. 2066.

U.S. government for implementing domestic nuclear detection efforts, as well as integration of federal nuclear forensics programs.

It should be noted that the SAFE Port Act has expired and is awaiting reauthorization.

Coast Guard Authorization Act of 2010

The Coast Guard Authorization Act of 2010 contains a number of provisions pertaining to maritime security. Section 811 of the Act creates a statutory requirement for FSPs to provide a system for seamen, pilots, and representatives of seamen's welfare and labor organizations to board and depart vessels through the facility in a timely manner at no cost to the individual. Section 821 of the Act charges the Secretary of the Department of Homeland Security to "establish comprehensive facility security officer training requirements designed to provide full security training that would lead to certification of such officers." The Act also calls for the development of provisional online training and a program of continuing education for FSOs and familiarization training for Federal, State, and local officials with security responsibilities at United States seaports.

Code of Federal Regulations

The rules contained in selected sections of the U.S. Code of Federal Regulations address maritime security. The focus of this part of the course should be to survey these regulations to provide trainees with knowledge of their location and an overview of their principal focus.

Instructors should survey the following regulations:

- 33 CFR Part 101 (Maritime Security, General)
- 33 CFR Part 103 (Area Maritime Security)
- 33 CFR Part 104 (Vessel Security)
- 33 CFR Part 105 (Facility Security)
- 33 CFR Part 106 (Outer Continental Shelf Facility Security)

In addition, the following CFRs are pertinent to facility security, and trainees should be aware of their existence and location:

- 33 CFR Part 126 (Handling Dangerous Cargo at Waterfront Facilities)
- 49 CFR Chapter 1 (Hazardous Materials Procedures and Regulations)
- 49 CFR Subchapter D (Maritime and Land Transportation Security)
- 49 CFR Parts 15 and 1520 (Protection of Sensitive Security Information)

49 CFR Parts 15 and 1520 contain the regulations concerned with the handling of Sensitive Security Information. This is a critically important subject for FSO trainees and is addressed in detail in a later section of the course.

2.4 U.S. Coast Guard directives, bulletins, and guidance

The instructor will identify for participants the various U.S. Coast Guard documents and sources that are used to convey information on maritime security within the agency and from the agency to the industry. The purpose of each should be briefly described. These include:

- Navigation and Vessel Inspection Circulars (NVICs)

- Maritime Security (MARSEC) Directives
- Commandant Instructions (COMDINSTs)
- Captain of the Port (COTP) orders
- ALDIST/ALCOAST bulletins
- PAC Decisions

2.5 Area Maritime Security

The Maritime Transportation Security Act of 2002 called for the development of AMSPs for each USCG COTP zone. Since that time, a comprehensive system of Area Maritime Security has evolved and is codified in 33 CFR Part 103.

Key elements of the Area Maritime Security system include the following:

1. Designation of the COTP in each zone as Federal Maritime Security Coordinator. The COTPs are the Federal Maritime Security Coordinators for their respective COTP zones.
2. Establishment of AMSCs in each COTP zone. Each AMSC is established under the direction of the cognizant COTP and shall assist in the development, review, and update of the AMSP for its area of responsibility. The AMSC is expected to:
   - Identify critical port infrastructure and operations;
   - Identify risks (threats, vulnerabilities, and consequences);
   - Determine mitigation strategies and implementation methods;
   - Develop and describe the process to continually evaluate overall port security by considering consequences and vulnerabilities, how they may change over time, and what additional mitigation strategies can be applied;
   - Provide advice to, and assist the COTP in, developing the AMSP; and
   - Serve as a link for communicating threats and changes in MARSEC Levels, and disseminating appropriate security information to port stakeholders.
3. Tasking each AMSC with ensuring that an Area Maritime Security Assessment (AMSA) is undertaken for its area of responsibility.
4. Requiring each COTP, in consultation with the AMSC, to develop an AMSP based on an AMSA that meets the provisions of Subpart D of Part 103. The AMSP must be consistent with the National Maritime Transportation Security Plan and the National Transportation Security Plan.
5. A requirement that the COTP coordinate with the AMSC to conduct or participate in an exercise at least once each calendar year, with no more than 18 months between exercises, to test the effectiveness of the AMSP. In some COTP zones, there are opportunities for FSOs to participate in the AMSC and the development of the AMSP.
6. It should be pointed out to trainees the entire AMSP is SSI and must be marked & protected accordingly.

2.6 Alternatives and equivalents

Recognizing that unusual or unique conditions may exist in individual facilities that render infeasible the strict application of the statutes as written, 33 CFR §105.140 provides for Alternative Security Programs (ASPs). In an ASP, a third party or industry organization

develops a standard that the Commandant then determines is able to provide a level of security equivalent to that established by Subchapter H.

Similarly, the regulations provide for the use of "Equivalent Security Measures." Under §101.130, a facility owner or operator may substitute an equivalent security measure that has been approved by the Commandant as meeting or exceeding the effectiveness of the required measure. The Commandant may require that the owner or operator provide data for use in assessing the effectiveness of the proposed equivalent security measure. Students should be aware of the procedures for requesting approval of equivalent security measures.

3. Facility Security Organization and Responsibilities

This section of the course is intended to give trainees an understanding of the various federal, state, and local agencies; other public and private entities; and individual security personnel who have authority or responsibilities involving maritime security. The impacts and duties of parties occupying specific roles within the system should be explained to students in the course.

3.1 Federal government agencies

The following Federal agencies regulate or otherwise impact facility security:

- Bureau of Alcohol, Tobacco, and Firearms
- Coast Guard
- Customs and Border Protection
- Department of Defense
- Department of Energy
- Department of Homeland Security
- Department of Justice
- Department of Transportation
- Environmental Protection Agency
- Federal Bureau of Investigation
- Federal Emergency Management Agency
- Food and Drug Administration
- Immigration and Customs Enforcement
- Maritime Administration
- Occupational Safety and Health Administration
- Transportation Security Administration

The instructor should summarize the jurisdictional authority of the federal agencies that affect marine terminal and regulated facility security, as appropriate. Strategies for FSO interaction with these agencies should be discussed.

3.2 State government agencies

State agencies that have a bearing on port and maritime security include the following:

- State departments of homeland security
- State police
- State Office of Emergency Management
- Port authorities (state-level)
- State departments of transportation
- Department of Natural Resources (or equivalent)
- Railroad Commission

The instructor should summarize the jurisdictional authority of the state agencies that affect regulated facility security. Strategies for FSO interaction with these agencies should be discussed.

3.3 Local government agencies

Local government and law enforcement agencies that affect security include:

- Sheriff's departments
- County police
- City police
- Port authorities (county- or city-level)

The instructor should summarize the jurisdictional authority of the local agencies that affect marine terminal and regulated facility security. Strategies for FSO interaction with these agencies should be discussed.

3.4 Jurisdictional issues

It should be pointed out to trainees that because there are often multiple government agencies involved in the administration of regulations pertaining to facility security, in some cases, this can result in overlapping or duplicative requirements. Strategies for dealing with these situations should be identified and discussed.

3.5 Owner or operator

The MTSA regulations define "owner or operator" as any person or entity that owns, or maintains operational control over, any facility, vessel, or OCS facility subject to Subchapter H.

Instructors should note that the FSO acts on behalf of the owner/operator in facility security matters and that from an operational standpoint, he or she is responsible for the security posture of the facility.

The instructor should highlight the requirements of 33 CFR §105.200 and Section 811 of the Coast Guard Authorization Act of 2010, which oblige the facility owner or operator to:

- Define the security organizational structure and provide each person exercising security duties and responsibilities within that structure the support needed to fulfill those obligations;

- Designate, in writing, by name or by title, an FSO and identify how the officer can be contacted at any time;
- Ensure that an FSA is conducted;
- Ensure the development and submission for approval of an FSP;
- Ensure that the facility operates in compliance with the approved FSP;
- Ensure that the TWIC program is properly implemented, including:
  - Ensuring that only individuals who hold a valid TWIC and are authorized to be in the secure/restricted area in accordance with the FSP are permitted to escort;
  - Identifying escort responsibilities and training; and
  - Notifying facility employees, and passengers if applicable, of what parts of the facility are secure areas and public access areas, as applicable, and ensuring such areas are clearly marked.
- Ensure that restricted areas are controlled and TWIC provisions are coordinated, if applied to such restricted areas;
- Ensure that adequate coordination of security issues takes place between the facility and vessels that call on it, including the execution of a Declaration of Security (DoS) as required by the regulations;
- Ensure that a system is provided for seamen assigned to a vessel at a port facility, pilots, and representatives of seamen's welfare and labor organizations to board and depart the vessel through the facility in a timely manner at no cost to the individual
- Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required for the new MARSEC Level;
- Ensure security for unattended vessels moored at the facility;
- Ensure the report of all breaches of security and transportation security incidents to the National Response Center in accordance with Part 101 of Subchapter H;
- Ensure consistency between security requirements and safety requirements;
- Inform facility personnel of their responsibility to apply for and maintain a TWIC, including the deadlines and methods for such applications, and of their obligation to inform TSA of any event that would render them ineligible for a TWIC, or which would invalidate their existing TWIC;
- Ensure that protocols consistent with 33 CFR §105.255(c), for dealing with individuals requiring access who report a lost, damaged, or stolen TWIC, or who have applied for and not yet received a TWIC, are in place; and
- If applicable, ensure that protocols consistent with 33 CFR §105.257, for dealing with newly hired employees who have applied for and not yet received a TWIC, are in place.

3.6 Facility Security Officer

33 CFR §105.205 delineates the role and duties of the FSO. The FSO has primary responsibility, on behalf of the owner or operator, for ensuring the security of the facility. Trainees should be made aware that the same person may serve as FSO for more than one facility, provided the facilities are in the same COTP zone and are not more than 50 miles apart. If a person serves as the FSO for more than one facility, the name of each facility for which he

or she is the FSO must be listed in the Facility Security Plan (FSP) of each facility for which he or she is the FSO.

§105.205 defines the responsibilities of the FSO as follows:

- Ensuring that the Facility Security Assessment (FSA) is conducted;
- Ensuring the development and implementation of an FSP;
- Ensuring that an annual audit is conducted and, if necessary, that the FSA and FSP are updated;
- Ensuring that the FSP is exercised per 33 CFR § 105.220;
- Ensuring that regular security inspections of the facility are conducted;
- Ensuring the security awareness and vigilance of the facility personnel;
- Ensuring adequate training of personnel performing facility security duties;
- Ensuring that occurrences that threaten the security of the facility are recorded and reported to the owner or operator;
- Ensuring the maintenance of records required by regulation;
- Ensuring the preparation and the submission of any reports required by regulation;
- Ensuring the execution of any required Declarations of Security with Masters, VSOs, or their designated representatives;
- Ensuring the coordination of security services in accordance with the approved FSP;
- Ensuring that security equipment is properly operated, tested, calibrated, and maintained;
- Ensuring the recording and reporting of attainment changes in MARSEC Levels to the owner or operator and the cognizant COTP;
- When requested, ensuring that VSOs receive assistance in confirming the identity of visitors and service providers seeking to board the vessel through the facility;
- Ensuring notification, as soon as possible, to law enforcement personnel and other emergency responders to permit a timely response to any transportation security incident;
- Ensuring that the FSP is submitted to the cognizant COTP for approval, as well as any plans to change the facility or facility infrastructure prior to amending the FSP;
- Ensuring that all facility personnel are briefed on changes in security conditions at the facility; and
- Ensuring that the TWIC program is being properly implemented.

3.7 Facility personnel with security duties

Trainees should learn that persons other than the FSO may be assigned specific security duties in connection with the FSP. The regulations contained in 33 CFR §105.210 require that facility personnel with designated security duties must maintain a TWIC, and must have knowledge of specific subjects that are enumerated in the discussion of training requirements later in this course.

3.8 All other facility personnel

A wide variety of personnel who do not have specific duties in connection with an FSP may have a positive impact on facility security. Facility personnel, whether full-time, part-time, permanent, or temporary, who do not have designated security duties under the FSP, are required by 33 CFR §105.215 to have knowledge of certain topics that are discussed in the training requirements section of this course.

Non-facility personnel visiting or working in the facility on a short-term basis, such as equipment technicians, classification society surveyors, ship chandlers, clergy, etc., may also be able to enhance facility security. Such persons should be provided on arrival with information on how to report suspicious activity or potentially dangerous situations.

3.9 Vessel security organization

FSO trainees should learn that SOLAS and certain other vessels have a Vessel Security Officer (VSO) ("Ship Security Officer" or "SSO" in international terminology) who has duties and responsibilities aboard his or her vessel that are similar to those of the FSO for the facility. Students should also be aware that there are vessel personnel who have duties in connection with the Vessel Security Plan (VSP) that are analogous to those of facility personnel with security duties. Vessel personnel who do not have designated security duties under the Vessel Security Plan are required to have knowledge of certain topics that are similar to those required of "all other facility personnel.

Finally, course participants should learn that non-vessel personnel visiting or working aboard a vessel on a short-term basis, such as equipment technicians, classification society surveyors, ship chandlers, clergy, etc., may also be able to enhance vessel and facility security.

4. Facility Security Measures

4.1 Physical security

Trainees should be familiar with the types of physical measures that can be used to enhance security in marine facilities, as appropriate, such as:

- Perimeter fencing
- Berms and Vehicle Barriers
- Blast walls
- Stand-offs
- Environmental design
- Signage
- Parking control
- Proximity controls

In particular, students should understand the effectiveness of a layered approach to physical security.

4.2 Access control

Students should be familiar with the provisions of 33 CFR §105.255 concerning access control, which require the facility owner or operator to ensure the implementation of security measures to:

- Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;
- Secure dangerous substances and devices that are authorized by the owner or operator to be on the facility;
- Control access to the facility; and
- Prevent an unescorted individual from entering an area of the facility that is designated as a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area.

The facility owner or operator must also ensure that the following are specified:

- The locations where restrictions or prohibitions that prevent unauthorized access are applied for each MARSEC Level, including those points where TWIC access control provisions will be applied. Each location allowing means of access to the facility must be addressed;
- The types of restrictions or prohibitions to be applied and the means of enforcing them;
- The means used to establish the identity of individuals not in possession of a TWIC, in accordance with §101.515, and procedures for escorting them;
- Procedures for identifying authorized and unauthorized persons at any MARSEC level; and
- The locations where screening of persons, personal effects and vehicles are to be conducted. The designated screening areas should be covered to provide for continuous operations regardless of the weather conditions.

Instructors should carefully clarify for trainees that the terms “secure” and “restricted” are used as defined in 33 CFR 101.105. It is important to ensure that areas that are designated “secure” and “restricted” for purposes of the regulations contained in Part 105 and the requirements of the TWIC program are not confused with secure and restricted areas established for other reasons or under other regulatory regimes.

TWIC Program

The requirements of the TWIC program are included under the topic of access control, and should be thoroughly explained to course participants. It should be explained that the facility owner or operator is obligated under 33 CFR §105.255 to ensure that the TWIC program is implemented as follows:

- All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access, in accordance with §101.514. Inspection must include:
  - A match of the photo on the TWIC to the individual presenting the TWIC;
  - Verification that the TWIC has not expired; and

- A visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.

- If an individual cannot present a TWIC because it has been lost, damaged or stolen, and he or she has previously been granted unescorted access to the facility and is known to have had a valid TWIC, the individual may be given unescorted access to secure areas for a period of no longer than 7 consecutive calendar days (see following paragraph for modification) if:
  - The individual has reported the TWIC as lost, damaged, or stolen to TSA as required in 49 CFR §1572.19(f);
  - The individual can present another identification credential that meets the requirements of §101.515; and
  - There are no other suspicious circumstances associated with the individual's claim of loss or theft.
- If an individual cannot present his or her TWIC for any other reason than outlined in paragraph (c)(2) of 33 CFR §105.255, he or she may not be granted unescorted access to the secure area. The individual must be under escort, as that term is defined in Part 101, at all times when inside of a secure area.
- With the exception of persons granted access according to paragraph (c)(2) of 33 CFR §105.255 all persons granted unescorted access to secure areas of the facility must be able to produce his or her TWIC upon request.
- There must be disciplinary measures in place to prevent fraud and abuse.
- The facility's TWIC program should be coordinated, when practicable, with identification and TWIC access control measures of vessels or other transportation conveyances that use the facility.

CG-FAC Policy Letter No. 12-04 dated 19 December 2012 modifies the above language in recognition of the fact that it is possible that an individual who has applied and paid for an initial TWIC, a TWIC renewal, or a person who has reported their TWIC as lost, stolen, or damaged will not receive it within 7 consecutive calendar days. To minimize disruptions of maritime operations and commerce, Owner/Operators of MTSA-regulated facilities may authorize unescorted access to an individual who has reported their TWIC to TSA as lost, damaged, or stolen and has yet to receive a replacement TWIC within 7 calendar days, an additional 30 calendar days for a total of 37 calendar days, This provision may also be extended to individuals who have applied for a TWIC renewal prior to its expiration, and through no fault of their own, are not able to take possession of their TWIC due to a significant delay in the application, production, issuance, and/or activation process. These accommodations are contingent upon specific conditions that are outlined in the policy letter.

Trainees should be advised that if the facility owner or operator uses a separate identification system, it must be consistent with the TWIC regulations.

The facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

Instructors should ensure that students are aware of the specific requirements pertaining to access control for each MARSEC level that are contained in §105.255 (f-h).

TWIC Escorting Requirements

Under the regulations as defined in 33 CFR §101.105, escorting means "ensuring that the escorted individual is continuously accompanied while within a secure area in a manner sufficient to observe whether the escorted individual is engaged in activities other than those for which escorted access was granted. This may be accomplished via having a side-by-side companion or monitoring, depending upon where the escorted individual will be granted access. Individuals without TWICs may not enter restricted areas without having an individual who holds a TWIC as a side-by-side companion, except as provided in §§ 104.267, 105.257, and 106.262 of this subchapter."

NVIC 03-07 provides additional guidance on escorting requirements and practices. As explained in this NVIC, escort requirements differ within secure areas depending on whether the area is also a restricted area or not. An individual not in possession of a TWIC who is authorized escorted access to a restricted area requires physical, side-by-side accompaniment by a TWIC holder. An individual not in possession of a TWIC who is authorized escorted access by the vessel or facility owner or operator to a secure area that is not also a restricted area requires monitoring in a manner sufficient to identify whether the individual is engaged in activities other than those for which escorted access was granted and that allows for quick response.

Enclosure (3) to NVIC 03-07 provides additional guidance on TWIC escorting requirements, including escorting ratios, monitoring issues, and related matters. Because of the importance of these provisions to the effective implementation of the TWIC program and preservation of facility security, instructors should carefully explain this material to trainees.

Public Access Areas

Trainees should be informed that the regulations in 33 CFR §105.106 provide that facilities serving ferries or passenger vessels certificated to carry more than 150 passengers, other than cruise ships, may designate an area within the facility as a public access area. This is a defined space within a facility that is open to all persons and provides pedestrian access through the facility from public thoroughfares to the vessel.

Shore Leave, Mariner Access, and Crewmember Detention

Sec 821 of the Coast Guard Authorization Act of 2010 requires that training "addresses requirements under the International Code for the Security of Ships and Port Facilities to address shore leave for mariners and access to visitors, representatives of seafarers' welfare organizations, and labor organizations."

It must be acknowledged that this has been a confusing and sometimes contentious issue in port and facility operations. Various countries and facilities within a given country have interpreted these requirements of the ISPS Code in quite different ways.

ISPS Code Part A 16.3.15 states that: "The plan shall address...procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship, including representatives of seafarers' welfare and labour organizations."

ISPS Code Part B 16.8.14 recommends that "In addition to the guidance given under paragraph 16.3, the PFSP should establish the following, which relate to all security levels...the procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship, including representatives of seafarers' welfare and labour organizations."

33 CFR 105.200 (b)(9) requires the facility owner or operator to: “Ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility for visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with vessel operators in advance of a vessel's arrival.”

In some cases, seafarers have been inappropriately confined to their vessels, have been charged exorbitant fees to be transported or escorted to and from the facility gate, and representatives of maritime labor and welfare organizations have been denied access to vessel personnel. As a result, the IMO has issued several circulars intended to clarify and reinforce the obligations of facilities and contracting governments to facilitate shore leave and to provide access to mariners by authorized organizations.

Instructors will need to refer to the most recent guidance by pertinent agencies—especially the Coast Guard—in advising trainees on how to address this issue. USCG ALCOAST Bulletin 575/09, in addressing this problem, notes a determination that the Coast Guard has the legal authority to mandate that MTSA-regulated facilities provide reasonable access to seafarers.

Section 811 of the Coast Guard Authorization Act of 2010 requires that approved FSPs “provide a system for seamen assigned to a vessel at that facility, pilots, and representatives of seamen’s welfare and labor organizations to board and depart the vessel through the facility in a timely manner at no cost to the individual.” Until such time as regulations implementing this language are in force, FSOs should be advised to work with their respective COTPs to resolve uncertainties associated with seafarer access and to ensure compliance with this requirement.

The most current guidance should also be obtained in those cases in which mariners are to be legitimately detained on board their ships. Trainees should be aware of the 2004 “Memorandum of Agreement between the Coast Guard and CBP Regarding the Detention of Certain High-Risk Crewmembers,” which provides standard operating procedures for coordinating efforts to identify high-risk foreign crewmembers and to ensure that effective security measures are put in place to prevent their illegal entry into the United States.

ALCOAST Bulletin 357/12, issued in August 2012, provides updates to processing policies made since the original publication of the 2004 USCG/CBP memorandum of agreement.

Railroad Operations

Railroad operations terminating in and transiting through the facility pose special challenges for access control. The operative guidance on this topic is found in PAC decisions 04-08 and 05-08. The latter states that facilities should work closely with security personnel from the railroads that service or cross their facility’s secure areas and that security measures for access control, as they relates to rail line access points, should be stated in procedures to be incorporated into the facility’s security plan.

Prospective FSOs should be advised that the principal concern is to ensure that the FSP reflects actions that are taken at each MARSEC level involving rail operations. The language in the FSP will vary depending upon the operation and upon the specific “alternatives and equivalents” approved by the Coast Guard. Individual operations will vary depending upon their location and the type of cargo handled.

4.3 Newly-hired employees

Trainees should be informed that the regulations in 33 CFR §105.257 require special handling of newly-hired employees where access control is concerned. Newly-hired facility employees may be granted entry to secure areas of the facility for up to 30 consecutive calendar days prior

to receiving their TWIC, provided all of the requirements in §105.257 (b) are met. If specific conditions are met, the new hire may be considered accompanied in his/her assigned work area. If TSA does not act upon a TWIC application within 30 days, the cognizant Coast Guard COTP may further extend access to secure areas for another 30 days. The Coast Guard will determine whether, in particular circumstances, certain practices meet the condition of a new hire being accompanied by another individual with a TWIC. Coast Guard guidance for use in making these determinations is contained in Enclosure (3) of NVIC 03-07. It should be noted that these provisions apply to direct employees of the facility only, and not to FSOs or persons with specific security duties.

4.4 Restricted areas

Restricted areas are discussed in 33 CFR §105.260. Facility owners or operators must ensure that restricted areas are designated within the facility. They must also ensure that all restricted areas are clearly marked and indicate that access to these areas is restricted and that unauthorized presence within the area constitutes a breach of security. The facility owner or operator may also designate the entire facility as a restricted area. Instructors should ensure that trainees are familiar with the delineation of restricted areas, understand which areas must be designated as restricted, recognize the required implementation of security measures associated with restricted areas at various MARSEC levels, as specified in §105.260.

4.5 Handling cargo

33 CFR §105.265 delineates regulatory requirements for the security measures that must be implemented in connection with cargo handling. Instructors should explain that the facility owner or operator must ensure that security measures relating to cargo handling (some of which may have to be applied in liaison with the vessel) are implemented in order to:

- Deter tampering;
- Prevent cargo that is not meant for carriage from being accepted and stored at the facility without the knowing consent of the facility owner or operator;
- Identify cargo that is approved for loading onto vessels interfacing with the facility;
- Include cargo control procedures at access points to the facility;
- Identify cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up;
- Restrict the entry of cargo to the facility that does not have a confirmed date for loading, as appropriate;
- Ensure the release of cargo only to the carrier specified in the cargo documentation;
- When there are regular or repeated cargo operations with the same shipper, coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedure; and
- Create, update, and maintain a continuous inventory of all dangerous goods and hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods and hazardous substances.

Trainees should also be made aware that there are specific requirements in 33 CFR §105.265 concerning handling cargo at each MARSEC level.

4.6 Delivery of vessel stores and bunkers

FSO course participants should be informed that operations involving the delivery of stores and bunkers impose specific obligations on the facility to ensure security. Under 33 CFR §105.270, the facility owner or operator is required to:

- Check vessel stores for package integrity;
- Prevent vessel stores from being accepted without inspection;
- Deter tampering;
- For vessels that routinely use a facility, establish and execute standing arrangements between the vessel, its suppliers, and a facility regarding notification and the timing of deliveries and their documentation; and
- Check vessel stores by the following means:
  - Visual examination;
  - Physical examination;
  - Detection devices, such as scanners; or
  - Canines.

Instructors should acquaint trainees with additional requirements concerning security measures for the delivery of stores and bunkers at different MARSEC levels detailed in §105.270.

4.7 Monitoring

Instructors should explain that the regulations require the facility owner or operator to ensure the implementation of security measures in 33 CFR §105.275 and to have the capability to continuously monitor, through a combination of lighting, security guards, waterborne patrols, automatic intrusion-detection devices, or surveillance equipment, as specified in the approved FSP, the facility and its approaches, on land and water; restricted areas within the facility; and vessels at the facility and areas surrounding the vessels.

Students should be referred to 33 CFR §105.275 to review the specific requirements for monitoring at each MARSEC level.

5. Security Technology and Cybersecurity

5.1 Types and functions of security equipment and systems

Course participants should be made aware of the types of security equipment and systems that are commonly used in the maritime environment. They should be cognizant of the fact that some of the most effective equipment used in facility security may be “low-tech,” as in the case where a simple fence excludes persons who might otherwise threaten the security of a facility.

Examples of the kinds of facility security equipment and systems that should be discussed, as appropriate, include:

- Alarms
- Baggage screening equipment

- Density meters
- Canines
- Closed Circuit Televisions (CCTV)
- Container X-ray devices
- Explosive detectors
- General alarm
- Handheld radios
- Key control
- Lighting
- Locks
- Metal detectors
- Patrol verification systems
- Perimeter Intrusion Detection Systems (microwave fence, buried cable, motion sensors)
- Radiation Portal Monitor (RPM)
- Sensors
- TWIC readers
- VACIS Inspection System
- Watch towers

Participants are not expected to acquire detailed technical or scientific knowledge concerning the theoretical underpinnings of the operation of security equipment. The objective is to ensure that trainees become familiar with the general capabilities and appropriate deployment of such devices and systems as are relevant to circumstances at their facilities.

5.2 Operational limitations of security equipment and systems

In this segment of the course, the functional limitations and operating constraints of security equipment and systems that FSOs may encounter or be called upon to use should be discussed. Issues such as effective range, environmental sensitivities, and operator (human) error should be addressed as appropriate.

5.3 Testing, calibration, and maintenance of security equipment and systems

Trainees should be familiar with methods for ensuring the continuing accuracy, efficiency, and operational readiness of selected items of security equipment and associated systems. FSO trainees should be able to describe maintenance procedures, calibration techniques, and test schedules for security equipment that may be used in the facility, as appropriate.

5.4 Evaluation and selection of facility security technology

The practicing FSO may well be in a position to influence the purchase and installation of facility security equipment and systems. Trainees should learn the importance of a systematic, needs-based assessment of facility security technology and equipment requirements. It should be

pointed out that an understanding of the purpose to be served by a particular item of equipment or system is an essential starting point. Security technology may be intended to deter, deny, detect, delay, or respond to attempts to breach facility security, or may offer some combination of these functions. It should also be emphasized that the choice of security equipment and systems should not be vendor-driven. The multiple costs associated with purchasing and deploying "technology in search of a problem" should be underscored by instructors.

5.5 Information assurance and cybersecurity

Modern facility operations are dependent to varying degrees on information systems that are often vulnerable to cyber threats. While the FSO function does not necessarily include direct responsibility for facility cybersecurity, trainees should be aware of the extent to which cargo and passenger operations rely upon information technology and the vulnerabilities associated with this technology. Awareness of the key principles of information system assurance is thus important. As appropriate, instructors should discuss such vulnerabilities as social engineering, weak passwords on internet-based CCTV systems, the compromise potential of industrial control systems, etc. Even the simplest operation has computer equipment such as a laptop that must be protected if the security of the facility is to be maintained.

6. Threat Recognition and Detection

6.1 Recognition and detection of dangerous substances and devices

The focus of this section of the course is on the characteristics and potential effects of weapons; explosives; chemical, biological, and radiological devices; substances and compounds that pose a hazard to personnel and/or vessels and facilities; and related topics.

Instructors should acquaint course participants with the basic appearance and effects of such weapons and substances as:

- Ammunition
- Automatic weapons
- Biological Weapons
- Chemical Weapons
- Illegal drugs
- Improvised Explosive Devices (IEDs)
- Knives
- Mace/pepper spray
- Man-Portable Air Defense Systems (MANPADS)
- Nuclear Weapons
- Pistols
- Radiological Weapons
- Rifles
- Rocket-Propelled Grenade Launchers (RPGs)

6.2 Recognition of persons posing potential security risks

Instructors should explain suspicious patterns of behavior, while emphasizing the importance of avoiding racial and ethnic stereotyping. Descriptions of suspicious activities such as those listed below should be discussed with course participants.

- Unauthorized persons photographing or filming the facility
- Unauthorized persons attempting to gain access to the facility
- Persons attempting to gain access to secure areas with improper or suspect identification, including fraudulent TWIC cards
- Individuals establishing businesses or roadside food stands in proximity to the facility
- Unauthorized persons loitering in the vicinity of the facility for extended periods of time
- Unauthorized persons phoning or e-mailing the facility to obtain information about facility operations
- Persons carrying on extended cell phone conversations in the facility vicinity
- Vehicles with personnel in them parked near the facility for extended periods
- Small boats with personnel on board loitering near the facility
- General aviation aircraft operating in the airspace above or near the facility
- Unknown persons attempting to acquire information the facility by engaging facility personnel or their families in a conversation.
- Vendors attempting to sell merchandise to facility personnel
- Unknown workmen trying to gain access to facilities to install or service equipment
- Unexpected package drop-offs or attempted drop-offs
- Anti-national pamphlets or flyers distributed to employees or placed on windshields in parking lots.
- Divers in the water near the facility
- Recreational boaters or persons aboard refugee craft posing as mariners in distress to attract assistance from the facility

6.3 Physical screening and non-intrusive inspections

The regulations contained in 33 CFR Subchapter H requires the screening of persons, cargo, vehicles, baggage, and stores at the rate specified in the approved FSP prior to allowing access to the facility. Instructors should emphasize to trainees that facility security personnel, unless sworn, do not exercise the powers of law enforcement officers where searches are concerned.

FSO certification based on this course requires practical demonstration of competence by trainees in procedures for physical screening. Procedures for assessment of competence established by the Coast Guard should be clearly explained to trainees.

The Coast Guard has provided guidance for developing and executing screening protocols that will be compliant with the access control provisions of Subchapter H. This information is contained in USCG NVIC 06-04 (“Voluntary Screening Guidance for Owners or Operators Regulated under Parts 104, 105, and 106 of Subchapter H of Title 33, Code of Federal Regulations”). Of particular relevance is Enclosure (1) to NVIC 06-04, which provides detailed

recommendations on screening policies and procedures. Enclosure (1) is SSI and must be protected accordingly.

6.4 Conducting security sweeps and searches

If temporary restricted areas are designated within the facility, 33 CFR §105.260 requires that the FSP must include a requirement to conduct a security sweep of the designated temporary restricted area both before and after the area has been established.

At MARSEC Level 3, searches of restricted areas may be specified in the approved FSP as part of a security sweep of all or part of the facility.

Trainees should be taught that search plans should be prepared in advance, to ensure that a thorough and efficient search is completed in the shortest possible time. The search plan should be comprehensive, and should detail the routes searchers should follow and the places on the route where weapons, devices, dangerous substances, etc. might be hidden.

The plan should be developed in a systematic manner to cover all options and to ensure no overlap or omission. This allows those responsible to concentrate on the actual search without worrying about missing something. Course participants should learn procedures to be followed so as to ensure effective and efficient searches.

6.5 Techniques used to circumvent security measures

Trainees should be cautioned that no security equipment or measure is infallible. They should be apprised of the known techniques that can be employed to evade security systems and controls, such as:

- Breaching of unmonitored perimeter barrier or waterside
- Bribing of facility personnel to obtain passwords
- Computer hacking
- Concealment in vehicles or containers
- Disabling CCTV cameras
- Disabling of alarm systems
- Disguise, deception, and diversion
- Falsification or alteration of TWIC cards
- Monitoring communications via scanner
- Radio-frequency jamming
- Use of bump keys

6.6 Internal conspiracies/sabotage

Course participants should be made aware of the challenges associated with internal conspiracies. An internal conspiracy is a situation in which trusted personnel of the facility, a vessel, or other entity with access to cargo moving through the supply chain or secure/restricted areas, motivated by greed, anger, political, or other factors, pose a security threat to the facility or port. The objective may be drug smuggling, cargo theft, insertion of WMD into a container, or other nefarious purpose.

Internal conspiracies and sabotage can be difficult activities to identify and address due to the level of criminal sophistication that is often possessed by those who engage in them. Such personnel often possess high-level information about facility and vessel operations, and may also have the ability to acquire and use complex technologies to avoid detection. Instructors should familiarize students with the principal types of internal criminal conspiracies and the actions that can be taken to prevent and detect them.

7. MARSEC Levels and Incident Response

7.1 MARSEC level coordination and implementation

MARSEC level coordination and implementation is addressed by 33 CFR §105.230. Trainees must be thoroughly familiar with the meaning of each MARSEC level. They must also learn who has the authority to change the MARSEC level at a facility and aboard a ship. The instructor should summarize the security measures that are associated with the various security levels that may be set. Regulatory requirements pertaining to coordination and implementation procedures at various MARSEC levels should be discussed.

Trainees should understand that facilities must be operated in compliance with the security requirements in §105.230 for the MARSEC level in effect for the port. When notified of an increase in the MARSEC level, the FSO, on behalf of the facility owner and operator, must ensure that:

- Vessels moored to the facility and vessels scheduled to arrive at the facility within 96 hours of the MARSEC level change are notified of the new MARSEC level and the Declaration of Security is revised as necessary;
- The facility complies with the required additional security measures within 12 hours; and
- The facility reports compliance or noncompliance to the COTP.

For MARSEC Levels 2 and 3, the Facility Security Officer must inform all facility personnel about identified threats, and emphasize reporting procedures and stress the need for increased vigilance.

The owner or operator of a facility that is not in compliance with the requirements of §105.230 must inform the COTP and obtain approval prior to interfacing with a vessel or continuing operations.

At MARSEC Level 3, in addition to the requirements in §105.230 a facility owner or operator may be required to implement additional measures pursuant to 33 CFR Part 6, 160, or 165, as appropriate, which may include but are not limited to:

- Use of waterborne security patrols;
- Use of armed security personnel to control access to the facility and to deter, to the maximum extent practical, a transportation security incident; and
- Examination of piers, wharves, and similar structures at the facility for the presence of dangerous substances or devices underwater or other threats.

An important objective of this section of the course is for trainees to understand the need to be familiar with, and adhere to, established procedures for interfacing with vessels at all MARSEC levels. Instructors should point out that the regulations require the facility owner or operator to ensure that there are measures in place for interfacing with vessels at all MARSEC levels.

7.2 The Declaration of Security (DoS)

The Declaration of Security (DoS) is discussed in 33 CFR §105.245. Course participants should learn that the DoS is an agreement executed between the FSO and a vessel's Master, VSO, or their designee that provides a means for ensuring that all shared security concerns are properly addressed and that security will remain in place throughout the time a vessel is moored to the facility or for the duration of the vessel-to-facility activity. Use of a DoS is required at all MARSEC levels when cruise ships and manned vessels subject to 33 CFR Part 104 carrying bulk CDC cargoes call at facilities regulated under 33 CFR Part 105. Before transferring passengers or cargo, other manned vessels regulated under Part 104 must complete a DoS when calling at a Part 105-regulated facility at MARSEC Levels 2 and 3.

Students should be familiar with the requirements pertaining to the DoS contained in 33 CFR §105.245, including the following:

Each facility owner or operator must ensure that procedures are established for requesting a DoS and for handling DoS requests from a vessel.

At MARSEC Level 1, a facility receiving a cruise ship or a manned vessel carrying Certain Dangerous Cargo, in bulk, must comply with the following:

- Prior to the arrival of a vessel to the facility, the FSO and the Master, VSO, or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of time the vessel is at the facility; and
- Upon the arrival of the vessel at the facility, the FSO and the Master, VSO, or their designated representatives, must sign the written DoS.

Neither the facility nor the vessel may embark or disembark passengers, nor transfer cargo or vessel stores until the DoS has been signed and implemented.

At MARSEC Levels 2 and 3, the FSOs, or their designated representatives, of facilities interfacing with manned vessels subject to 33 CFR Part 104 must sign and implement DoSs as required in (b)(1) and (2) of §105.245.

At MARSEC Levels 1 and 2, FSOs of facilities that frequently interface with the same vessel may implement a continuing DoS for multiple visits, provided that:

- The DoS is valid for a specific MARSEC Level;
- The effective period at MARSEC Level 1 does not exceed 90 days; and
- The effective period at MARSEC Level 2 does not exceed 30 days.

When the MARSEC level increases beyond that contained in the DoS, the continuing DoS is void and a new DoS must be executed.

A copy of all currently valid continuing Declarations of Security must be kept with the FSP.

The COTP may require, at any time, at any MARSEC level, any facility subject to Part 105 to implement a DoS with the VSO prior to any vessel-to-facility interface when he or she deems it necessary.

7.3 Security incident responsibilities

33 CFR §105.280 delineates security incident responsibilities of the FSO and facility security personnel. Instructors should familiarize students with the requirements at each MARSEC level for FSOs and facility security personnel to be able to:

- Respond to security threats or breaches of security and maintain critical facility and vessel-to-facility interface operations;
- Evacuate the facility in case of security threats or breaches of security;
- Report security incidents as required by regulations;
- Brief all facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and
- Secure non-critical operations in order to focus response on critical operations.

7.4 Security-related communications

33 CFR §105.235 discusses communications. Instructors should advise trainees that the FSO must have a means to effectively notify facility personnel of changes in security conditions at the facility. Communication systems and procedures must allow effective and continuous communications between facility security personnel, vessels interfacing with the facility, the cognizant COTP, and national and local authorities with security responsibilities. At each active facility access point, a means of communication must be provided for contacting police, security control, or an emergency operations center, by telephones, cellular phones, and/or portable radios, or other equivalent means. Students should learn that facility communications systems must have redundancy for both internal and external communications.

7.5 Reporting security incidents

Instructors will inform students that owners/operators and FSOs of MTSA-regulated facilities are required to promptly report activities that may result in a TSI by telephone to the U.S. Coast Guard National Response Center in accordance with 33 CFR §101.305. Similarly, breaches of security must also be reported to the National Response Center via telephone.

If a TSI occurs, the regulations require the owner or operator to report it to their local COTP and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the National Response Center.

Callers to the National Response Center should be prepared to provide as much of the following information as possible:

- Their own name and contact information;
- The name and contact information of the suspicious or responsible party;
- The location of the incident, as specifically as possible; and
- The description of the incident or activity involved.

7.6 Interfacing with first responders

Central to effective incident response in ports and maritime facilities is the interface between facility personnel and first responders such as fire-fighters and police officers. Instructors should ensure that prospective FSOs are aware of Incident Command System (ICS) protocols that are used by first responders in emergency situations. The importance of having and adhering to established procedures for interfacing with first responders in a crisis should be emphasized.

ICS is a subset of the National Incident Management System (NIMS), which is a comprehensive, national framework that provides the template for incident management, regardless of cause, size, location, or complexity. ICS is a standardized, on-scene, all-hazards approach that: (1) allows for the integration of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure; (2) enables a coordinated response among various jurisdictions and functional agencies, both public and private; and (3) establishes common processes for planning and managing resources. ICS is flexible and can be used for incidents of any type, scope, and complexity. ICS allows its users to adopt an integrated organizational structure to match the complexities and demands of single or multiple incidents.

7.7 Evacuation of the facility

Trainees should understand the need for all facility personnel to know the location of their muster stations and escape and evacuation routes from the facility. The need for practice of facility evacuation through regular drills and exercises should be underscored. Students should also be made aware that, in some emergencies, it may be safer to shelter in place than to leave the facility. Instructors should also discuss the fact that in some circumstances, partial evacuation of the facility may be advisable.

7.8 Emergency Operations Plan (EOP)

Successful response to crises at a facility may be dependent on the existence and implementation of an Emergency Operations Plan (EOP). This plan defines how the facility will operate during and after an incident, and may address such topics as:

- Chain of command and responsibilities
- Emergency Operations Center (EOC) location and operations
- Emergency communications
- Evacuation procedures and sheltering in place
- Emergency operations
- Damage assessment
- Disaster recovery
- Insurance claims
- Personnel management
- Financial issues
- Public affairs
- Relief operations support

Course participants should understand the concept of resilience as applied to port and facility operations. DHS has defined resilience as "[the] ability of systems, infrastructures, government, business, communities, and individuals to resist, tolerate, absorb, recover from, prepare for, or adapt to an adverse occurrence that causes harm, destruction, or loss."[3]

The pivotal importance of the marine transportation system to the U.S. economy and the national defense makes it essential that disruptions to facility operations be minimized. The more resilient a facility is, the more rapidly it can resume handling cargo, moving passengers, or facilitating sealift operations, as the case may be.

8. Security Training, Drills, and Exercises

8.1 Training requirements

Early in the course, students should have been familiarized with the subjects in which FSOs are required to be trained, as listed in 33 CFR §105.205.

33 CFR §105.210 defines knowledge requirements for facility personnel with security duties. Instructors should summarize for course participants the topics that are the focus of training for personnel in this category, who must have knowledge in the following areas, as appropriate:

- Knowledge of current security threats and patterns;
- Recognition and detection of dangerous substances and devices;
- Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
- Techniques used to circumvent security measures;
- Crowd management and control techniques;
- Security related communications;
- Knowledge of emergency procedures and contingency plans;
- Operation of security equipment and systems;
- Testing, calibration, and maintenance of security equipment and systems;
- Inspection, control, and monitoring techniques;
- Relevant provisions of the FSP;
- Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores;
- The meaning and the consequential requirements of the different MARSEC Levels; and
- Relevant aspects of the TWIC program and how to carry them out.

In addition, knowledge of certain maritime security awareness topics is required by 33 CFR §105.215 of all other facility personnel. All other facility personnel, including contractors, whether part-time, full-time, temporary, or permanent, must have knowledge of, through training or equivalent job experience, of the following subjects, as appropriate:

- Relevant provisions of the FSP;

[3] DHS Risk Lexicon—2010 Edition. http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf. 26

- The meaning and the consequential requirements of the different MARSEC Levels as they apply to them, including emergency procedures and contingency plans;
- Recognition and detection of dangerous substances and devices;
- Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
- Techniques used to circumvent security measures; and
- Relevant aspects of the TWIC program and how to carry them out.

FSO trainees should be made aware of the importance to facility security of ongoing professional development and knowledge acquisition. In addition to ensuring that knowledge and skills remain "fresh," revisions to regulations, developments in technology, and other changes make it imperative that security training be viewed as a continuous process.

8.2 Instructional techniques

Given that the FSO carries the burden of ensuring that proper training in the appropriate subjects has been provided to personnel responsible for the security of the facility, trainees should be exposed to practical instructional techniques. This information can be used directly by the FSO in the role of instructor or may be employed in evaluating training programs being used by, or being considered for use, by the facility.

8.3 Requirements for security drills and exercises

The regulations concerning drills and exercises are found in 33 CFR §105.220. It should be conveyed to participants in the FSO course that the objectives of drills and exercises are to ensure that facility personnel are proficient in all assigned security duties at all security levels and to test the effective implementation of the FSP. Drills and exercises should enable the FSO to identify any security-related deficiencies that need to be addressed.

It should be emphasized to trainees that properly conducted drills and exercises are essential to the maintenance and enhancement of facility security. Both official analyses and anecdotal evidence suggest that compliance with drill and exercise requirements is a frequent source of facility security inspection deficiencies.

A drill is defined by the regulations as a training event that tests at least one component of a security plan, and which is used to maintain a high level of security readiness. It should be noted that a drill or exercise required by §105.220 may be satisfied with the implementation of security measures required by the FSP as the result of an increase in the MARSEC level, provided the facility reports attainment to the cognizant COTP.

The FSO must ensure that at least one security drill is conducted every three months. Security drills may be held in conjunction with non-security drills, where appropriate. Drills must test individual elements of the FSP, including response to security threats and incidents. Drills should take into account the types of operations of the facility, facility personnel changes, the type of vessel the facility is serving, and other relevant circumstances. Examples of drill scenarios include unauthorized entry to a restricted area, response to alarms, and notification to law enforcement authorities of a TSI.

If a vessel is moored at the facility on the date the facility has planned to conduct a drill, the facility cannot require the vessel or vessel personnel to participate in the facility's scheduled drill. However, a vessel may welcome the opportunity to engage in a facility security drill.

Students must learn that exercises are more extensive and comprehensive than drills. An exercise involves a full test of the functional elements of a security plan, including communications, coordination, resource availability, and response. Exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

Exercises may be of the following types:

- Full scale or live;
- Tabletop simulation or seminar;
- Combined with other appropriate exercises; or
- A combination of the exercise types listed above.

Exercises may be facility-specific or part of a cooperative exercise program with applicable FSPs and VSPs or comprehensive port exercises. Exercises must include substantial and active participation of FSOs, and may include government authorities and vessels visiting the facility. Requests for participation of CSOs and VSOs in joint exercises should consider the security and work implications for the vessel(s) involved.

8.4 Assessment of security drills and exercises

Participants should learn that at the end of each drill or exercise, the FSO should review the drill or exercise, and ensure that any mistakes made or deficiencies that have been identified are corrected. All personnel involved should give their comments on the effectiveness of the drill to the FSO, who is responsible for ensuring that facility personnel understand their security responsibilities and are properly trained to carry them out.

The post-drill or post-exercise “hot wash” should be aimed at identifying best practices and lessons learned as well as resolutions for identified deficiencies, which should be carefully documented by the FSO.

The development by the FSO of standards or performance metrics against which the effectiveness of drills and exercises can be assessed should be encouraged by instructors.

9. Security Administration

9.1 Handling Sensitive Security Information (SSI)

The principal regulations pertaining to SSI materials are found in 49 CFR Parts 15 and 1520. Trainees need to acquire a sense of the critical importance of properly handling documents and information that are considered SSI. Instructors need to explain to trainees that the FSA, FSA report, and FSP are SSI and must be marked and protected from unauthorized access or disclosure. The potential consequences of unintended disclosure of, or unauthorized access to, such material as the FSA or the FSP should be emphasized. Instructors should place heavy emphasis on the specific regulatory provisions concerning who should be given access to SSI, how it should be stored and secured, and appropriate means for its transmission.

Instructors may wish to utilize Coast Guard NVIC 10-04 as a guide for discussion on this topic. NVIC 10-04 is titled “Guidelines for Handling of Sensitive Security Information (SSI).” Enclosures (1) – (5) of the NVIC clarify the nature of SSI and discuss its appropriate handling in detail. Regulatory references are also provided by the NVIC.

It should be pointed out by instructors that careless handling of SSI can easily compromise the security of the facility and put its personnel and assets at grave risk. In addition, it should be noted that the law provides for significant penalties in cases where disclosure of SSI to

unauthorized parties occurs. Trainees should also be aware of the regulatory requirement that when a covered person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly inform TSA or the applicable DOT or DHS component or agency.

9.2 Documentation and record retention

Facility recordkeeping requirements are defined in 33 CFR §105.225. Students should be advised that the regulations require the FSO to keep records of the activities listed below for at least two years and that they must be made available to the Coast Guard upon request. If these records are kept in electronic format, they must be protected against unauthorized deletion, destruction, or amendment. These records must be protected from unauthorized access or disclosure. The following records must be kept:

- **Training**. For training under §105.210, the date of each session, duration of session, a description of the training, and a list of attendees;
- **Drills and exercises**. For each drill or exercise, the date held, description of drill or exercise, list of participants, and any best practices or lessons learned which may improve the FSP;
- **Incidents and breaches of security**. For each incident or breach of security, the date and time of occurrence, location within the facility, description of incident or breaches, to whom it was reported, and description of the response;
- **Changes in MARSEC Levels**. For each change in MARSEC Level, the date and time of notification received, and time of compliance with additional requirements;
- **Maintenance, calibration, and testing of security equipment**. For each occurrence of maintenance, calibration, and testing, record the date and time, and the specific security equipment involved;
- **Security threats**. For each security threat, the date and time of occurrence, how the threat was communicated, who received or identified the threat, description of threat, to whom it was reported, and description of the response;
- **Declaration of Security**. A copy of each single-visit DoS and a copy of each continuing DoS for at least 90 days after the end of its effective period; and
- **Annual audit of the FSP**. For each annual audit, a letter certified by the FSO stating the date the audit was completed.

9.3 Facility security force management

As appropriate, instructors should acquaint prospective FSOs with the various ways in which facility security forces can be structured. The advantages and disadvantages of proprietary versus contract security personnel should figure prominently in this discussion. The existence of sworn officers in some ports should be noted. Implications of the decision as to whether to build and manage an “in-house” security force or to contract with an outside security firm include factors of cost, liability, administrative workload, labor-management relations, and other issues.

Trainees should understand the basic parameters of security force operations. Instructors should discuss such elements as security patrols, command center functions, use of security equipment, uniforms, K-9 teams, monitoring, shift scheduling, supervision, report writing, the use of logs, communications, etc.

Trainees should learn that systematic recruiting and pre-employment screening are important factors in the development of an effective security force. The use of established Human Resources practices in this regard is imperative. The development of comprehensive position descriptions is an essential first step. Interviews, criminal record checks, prior employment verification, reference checks, drug tests, and related actions are important in ensuring that qualified, responsible, and professional security personnel are hired.

Once hired, security personnel require proper training which, at a minimum, addresses the knowledge and skill requirements contained in 33 CFR §105.210. Beyond this, the nature of operations and the particular challenges at individual facilities will often make facility-specific training necessary. The owner or operator of a cruise terminal, for example, will likely require security personnel to have specific training that will enable the facility to provide maximum protection to cruise passengers and their possessions.

FSOs should learn that there are a number of liability concerns relating to facility security personnel and their actions. Litigation may arise as a result of screening activities, use of force, seizure, work-related injuries, disruption of cargo operations, and other triggers.

10. Facility Security Assessment (FSA)

10.1 Risk assessment methods

Facility security assessment is the foundation of an effective security system. It is an integral part of the process of developing and updating the Facility Security Plan. Trainees should learn that multiple risk assessment models and methods exist, and that some of them are not appropriate for use in facility security. A key point is that whatever approach is adopted by a particular facility, a thorough understanding of its benefits, limitations, and correct application is essential. Students should realize that a systematic and organized approach to facility security assessment is critically important to the preservation and enhancement of security. Such an approach should be central in the completion of security assessments and in the determination of appropriate security measures for the facility.

One example of a risk assessment method that can be presented to students is Risk Based Decision Making (RBDM). RBDM is a methodical and analytical process used to identify threats, determine the probability and consequences of incidents that may result from those threats, document vulnerabilities that may lead to increased risk, and develop counter-strategies and mitigations to eliminate or reduce the impact of identified threats.

Generally, RBDM is undertaken by completing these steps:

- Step 1: Establish the decision structure
- Step 2: Perform the risk assessment
- Step 3: Apply the results to risk management decision making
- Step 4: Monitor effectiveness through impact assessment
- Step 5: Facilitate risk communication

Risk Based Decision Making as applied to facility security assessment is described in Enclosure (1) to USCG NVIC 11-02, Change 1, as follows:

> Risk-based decision-making is one of the best tools to perform a security assessment and to determine appropriate security measures for a facility. Risk-based decision-making is a systematic and analytical process to consider the likelihood that a security breach will endanger an asset, individual, or function

and to identify actions that will reduce the vulnerability to and mitigate the consequences of a security breach.

A security assessment is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may lead to a security breach, and may suggest options to eliminate or mitigate those weaknesses. For example, a security assessment might reveal weaknesses in an organization's security systems or underprotected access points such as the facility's perimeter not being lighted or gates not being secured or monitored after hours. To mitigate this vulnerability, a facility would implement procedures to ensure that such access points are appropriately secured and verified by some means. Another security enhancement might be to place locking mechanisms and/or wire mesh on doors and windows that provide access to restricted areas to prevent unauthorized personnel from entering such spaces. Such assessments can identify vulnerabilities in facility operations, personnel security, and physical and technical security.

Detailed guidance on application of the RBDM framework to facility security assessment is given in NVIC 11-02, Change 1. Trainees may be advised to utilize this NVIC as a source of guidance on the risk analysis process. However, it is important to emphasize that there are many ways in which to analyze threats, vulnerabilities, and the consequences of security incidents. The RBDM approach is only one example.

10.2 Facility Security Assessment requirements

Trainees must be informed of the general requirements in 33 CFR Part 105 Subpart C concerning the FSA. It should be noted the FSA is a written document that is based on the collection of background information, the completion of an on-scene survey, and an analysis of the results of these efforts.

Trainees should also be informed that the regulations allow for the involvement of third parties in any aspect of the FSA if they have the appropriate skills and if the FSO reviews and accepts their work. This underscores the importance of FSO competence in the FSA process, even if other parties are retained to conduct the FSA and/or to develop the FSP. Instructors should clarify the role of third parties in the FSA process. Those involved in the FSA process must be able to draw upon expert assistance in the completion and updating of the FSA, primarily because there are many different facets of facility operations and security and no single person can possess in-depth knowledge in all of these areas.

Third parties furnishing expert advice who are consulted in connection with an FSA may be called upon to provide expertise in any of the following subjects:

- Knowledge of current security threats and patterns;
- Recognition and detection of dangerous substances and devices;
- Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
- Techniques used to circumvent security measures;
- Methods used to cause a security incident;
- Effects of dangerous substances and devices on structures and facility services;
- Facility security requirements;
- Facility and vessel interface business practices;

- Contingency planning, emergency preparedness, and response;
- Physical security requirements;
- Radio and telecommunications systems, including computer systems and networks;
- Marine or civil engineering; and
- Facility and vessel operations.

10.3 Background

Trainees should be familiar with the background information that should be provided to the person or persons who will conduct the assessment. As defined in 33 CFR §105.305(a), this information includes, as applicable, the following:

- The general layout of the facility, including:
  - The location of each active and inactive access point to the facility;
  - The number, reliability, and security duties of facility personnel;
  - Security doors, barriers, and lighting;
  - The location of restricted areas;
  - The emergency and stand-by equipment available to maintain essential services;
  - The maintenance equipment, cargo spaces, storage areas, and unaccompanied baggage storage;
  - Location of escape and evacuation routes and assembly stations; and
  - Existing security and safety equipment for protection of personnel and visitors;
- Response procedures for fire or other emergency conditions;
- Procedures for monitoring facility and vessel personnel, vendors, repair technicians, and dock workers;
- Existing contracts with private security companies and existing agreements with local or municipal agencies;
- Procedures for controlling keys and other access prevention systems;
- Procedures for cargo and vessel stores operations;
- Response capability to security incidents;
- Threat assessments, including the purpose and methodology of the assessment, for the port in which the facility is located or at which passengers embark or disembark;
- Previous reports on security needs; and
- Any other existing security procedures and systems, equipment, communications, and facility personnel.

Students should be advised that the active collection of information regarding potential threats to the security of the facility can add value in the risk assessment process. This requires the development of a structured and effective program to gather and to effectively utilize intelligence. The FSO may be able to draw relevant information from the following sources:

- Unclassified government-managed intelligence information, including reports generated by military and law enforcement agencies
- Open source information such as newspapers, journals, trade publications, etc.

- In-house intelligence operations, which may acquire and analyze intelligence information from informants and personnel in the local community.

10.4 On-scene security surveys

Instructors should explain that the facility owner or operator must ensure that an on-scene survey of each facility is conducted in accordance with 33 CFR §105.305(b). The on-scene survey involves the examination and evaluation of facility protective measures, procedures, and operations in order to collect and verify the background information described above.

10.5 Analysis and recommendations

Trainees should become familiar with the process of analyzing background information and the results of the on-scene survey to develop recommendations that establish and prioritize the security measures that should be included in the FSP, as required by 33 CFR §105.305(c). The analysis must consider:

- Each vulnerability found during the on-scene survey including but not limited to:
  - Waterside and shore-side access to the facility and vessel berthing at the facility;
  - Structural integrity of the piers, facilities, and associated structures;
  - Existing security measures and procedures, including identification systems;
  - Existing security measures and procedures relating to services and utilities;
  - Measures to protect radio and telecommunication equipment, including computer systems and networks;
  - Adjacent areas that may be exploited during or for an attack;
  - Areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations within the facility;
  - Existing agreements with private security companies providing waterside and shore-side security services;
  - Any conflicting policies between safety and security measures and procedures;
  - Any conflicting facility operations and security duty assignments;
  - Any enforcement and personnel constraints;
  - Any deficiencies identified during daily operations or training and drills; and
  - Any deficiencies identified following security incidents or alerts, the report of security concerns, the exercise of control measures, or audits;
- Possible security threats, including but not limited to:
  - Damage to or destruction of the facility or of a vessel moored at the facility;
  - Hijacking or seizure of a vessel moored at the facility or of persons on board;
  - Tampering with cargo, essential equipment or systems, or stores of a vessel moored at the facility;
  - Unauthorized access or use including the presence of stowaways;
  - Smuggling dangerous substances and devices to the facility;
  - Use of a vessel moored at the facility to carry those intending to cause a security incident and their equipment;
  - Use of a vessel moored at the facility as a weapon or as a means to cause damage or destruction;

  - Impact on the facility and its operations due to a blockage of entrances, locks, and approaches; and
  - Use of the facility as a transfer point for nuclear, biological, radiological, explosive, or chemical weapons;
- Threat assessments by government agencies;
- Vulnerabilities, including human factors, in the facility's infrastructure, policies and procedures;
- Any particular aspects of the facility, including the vessels using the facility, which make it likely to be the target of an attack;
- Likely consequences in terms of loss of life, damage to property, and economic disruption, including disruption to transportation systems, of an attack on or at the facility; and
- Locations where access restrictions or prohibitions will be applied for each MARSEC Level.

10.6 FSA Report

The purpose of the FSA report should be communicated to trainees. The FSA report is a detailed summary of the results of the FSA and becomes an element of the FSP. Instructors should explain that under the requirements of 33 CFR §105.305(d), the facility owner or operator must ensure that a written FSA report is prepared and included as part of the FSP. The report must contain:

- A summary of how the on-scene survey was conducted;
- A description of existing security measures, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems;
- A description of each vulnerability found during the on-scene survey;
- A description of security measures that could be used to address each vulnerability;
- A list of the key facility operations that are important to protect; and
- A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the facility.

The FSA report must describe the following elements within the facility:

- Physical security;
- Structural integrity;
- Personnel protection systems;
- Procedural policies;
- Radio and telecommunication systems, including computer systems and networks;
- Relevant transportation infrastructure; and
- Utilities.

The FSA report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:

- Facility personnel;

- Passengers, visitors, vendors, repair technicians, vessel personnel, etc.;
- Capacity to maintain emergency response;
- Cargo, particularly dangerous goods and hazardous substances;
- Delivery of vessel stores;
- Any facility security communication and surveillance systems; and
- Any other facility security systems, if any.

The FSA report must account for any vulnerabilities in the following areas:

- Conflicts between safety and security measures;
- Conflicts between duties and security assignments;
- The impact of watch-keeping duties and risk of fatigue on facility personnel alertness and performance;
- Security training deficiencies; and
- Security equipment and systems, including communication systems.

The FSA report must discuss and evaluate key facility measures and operations, including:

- Ensuring performance of all security duties;
- Controlling access to the facility, through the use of identification systems or otherwise;
- Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);
- Procedures for the handling of cargo and the delivery of vessel stores;
- Monitoring restricted areas to ensure that only authorized persons have access;
- Monitoring the facility and areas adjacent to the pier; and
- The ready availability of security communications, information, and equipment.

10.7 Submission Requirements

Instructors should explain the requirements for submission of the FSA report as contained in 33 CFR §105.310. It should be emphasized that a completed FSA report must be submitted with the FSP. It should be noted that a facility owner or operator may generate and submit a report that contains the FSA for more than one regulated facility, to the extent that the facilities are of similar design and operation, if authorized and approved by the cognizant COTP. Finally, trainees must be informed that the FSA must be reviewed and validated, and that the FSA report must be updated each time the FSP is submitted for reapproval or revisions.

11. Facility Security Plan (FSP)

11.1 Facility Security Plan requirements

The FSO is required by 33 CFR §105.400 to ensure that an FSP is developed and implemented for each facility for which he or she is designated as FSO. The FSP:

- Must identify the FSO by name and position, and provide 24-hour contact information;
- Must be written in English;

- Must address each vulnerability identified in the FSA;
- Must describe security measures for each MARSEC level; and
- May cover more than one facility to the extent that they share similarities in design and operations, if authorized and approved by the cognizant COTP.

11.2 Format and content of the FSP

Trainees should understand the requirement that the FSP describe in detail how the requirements contained in 33 CFR Part 105 Subpart B will be met. Instructors should note that 33 CFR §105.405 charges facility owners or operators with ensuring that the FSP includes all of the following 18 sections:

1. Security administration and organization of the facility;
2. Personnel training;
3. Drills and exercises;
4. Records and documentation;
5. Response to change in MARSEC Level;
6. Procedures for interfacing with vessels;
7. Declaration of Security (DoS);
8. Communications;
9. Security systems and equipment maintenance;
10. Security measures for access control, including designated public access areas;
11. Security measures for restricted areas;
12. Security measures for handling cargo;
13. Security measures for delivery of vessel stores and bunkers;
14. Security measures for monitoring;
15. Security incident procedures;
16. Audits and security plan amendments;
17. Facility Security Assessment (FSA) report; and
18. Facility Vulnerability and Security Measures Summary (Form CG–6025).

If the sections of a particular FSP are not organized in the order given in the list above, the facility owner or operator must ensure that the FSP contains an index identifying the location of each section in the plan.

11.3 Submission and approval of the FSP

Trainees need to learn that all facilities subject to 33 CFR Part 105 must submit completed FSPs in accordance with 33 CFR §105.310, 33 CFR §105.410 and, if applicable, HOMEPORT. The FSP must be submitted for approval in written or

electronic format. FSPs should be submitted to the cognizant COTP, via the closest Coast Guard Marine Safety Unit, Marine Safety Detachment, or Sector Field Office; or as directed by the COTP. An FSA must be submitted with each FSP along with a letter certifying that the FSP has met the requirements of 33 CFR 105.

After an initial screening is completed, plans undergo an initial review to ensure that the 18 basic required sections are properly included and addressed. If major deficiencies are identified during this review, the plan must be corrected and resubmitted. Major deficiencies include: (1) an incomplete or missing Form CG-6025, (2) an incomplete or missing FSA report, and/or (3) two or more incomplete FSP content requirements.

The principal actions that may be taken by the Coast Guard following receipt of a submitted FSP are:

- Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;
- Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or
- Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

Trainees should be directed to review the detailed flow chart depicting the submission/approval process contained in Enclosure (1) to NVIC 03-03, Change 2.

11.4 Amendment and audit of the FSP

The regulations concerned with amendment and audit of the FSP are found in 33 CFR §105.415. Key provisions should be reviewed with course participants.

Provisions concerning amendments to the FSP include the following:

- Amendments to a FSP that has been approved by the cognizant COTP may be initiated by the facility owner or operator or the COTP upon a determination that an amendment is needed to maintain the facility's security. Proposed amendments must be submitted to the COTP.

- If initiated by the COTP, the facility owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the facility owner or operator shall ensure temporary security measures are implemented to the satisfaction of the COTP.

- If initiated by the facility owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the COTP allows a shorter period. The COTP will approve or disapprove the proposed amendment in accordance with §105.410.

- These requirements are not intended to deter the facility owner or operator from timely implementation of such additional security measures not enumerated in the approved FSP as may be necessary to address exigent security situations. In such cases, the

owner or operator must notify the COTP as quickly as possible concerning the nature of the additional measures, the circumstances that prompted these additional measures, and the period of time these additional measures are expected to be in place.

As noted in NVIC 03-03, Change 2, administrative changes, such as new phone numbers or a change in the name of the FSO or Alternate FSO must be noted on the FSP and forwarded to the COTP, but do not require a new FSA or amendments to the FSP.

Provisions concerning audits of the FSP include the following:

- The FSO must ensure that an audit of the FSP is performed annually, beginning no later than one year from the initial date of approval, and attach a letter to the FSP certifying that the FSP meets applicable requirements.
- The FSP must be audited if there is a change in the facility's owner or operator, or if there have been modifications to the facility involving such elements as physical structure, emergency response procedures, security measures, or operations.
- Audits of the FSP as a result of modifications to the facility may be limited to those sections of the FSP affected by the facility modifications.
- Unless impracticable due to the size and nature of the company or the facility, personnel conducting internal audits of the security measures specified in the FSP or evaluating its implementation must (1) have knowledge of methods for conducting audits and inspections, and security, control, and monitoring techniques; (2) not have regularly assigned security duties; and (3) be independent of any security measures being audited.
- If the results of an audit require amendment of either the FSA or FSP, the FSO must submit the proposed amendment(s) to the COTP for review and approval no later than 30 days after completion of the audit and a provide a letter certifying that the amended FSP meets applicable requirements

Instructors should distinguish for trainees the differences between internal and external audits and note the critical importance of ensuring that auditors, whether internal or external, are fully qualified to undertake audit responsibilities. Trainees should also be advised that, as FSOs, they should retain copies of all audit and amendment documents.

Students should review Enclosure (8) to NVIC 03-03, Change 2, which provides guidance on facility security audits and a sample audit report form. As noted in Enclosure (8), the intent of the regulation and the purpose of an audit are to identify opportunities for improvement and to address non-conformities. An audit accomplishes this through the review of facility operations and the implementation of corrective actions that ensure regulatory compliance and preclude the recurrence of deficiencies.

Enclosure (8) also notes that several opportunities exist for the auditor to analyze the effectiveness of the regulated entity in implementing the FSP. For example, a review of quarterly drills, annual exercises, and corrective action following a deficiency or recorded security event (such as a security incident or breach of security) provides an auditor the chance to see the plan operate and to learn how it is improved. An effective audit might include site visits to the facility at various times of the day and night; interviews with and observation of personnel performing security duties; review of and observation of security procedure

implementation; verification of the operability, testing, and planned maintenance of security equipment; examination of documentation, and performance verification of required training.

11.5 Use of Form CG-6025 or subsequent version

Instructors should explain that the Facility Vulnerability and Security Measures Summary (Form CG–6025) must be completed using information in the FSA report as required by 33 CFR §105.405(c). The CG-6025 is prepared based on material contained in the FSA report that provides key information about the facility, identifies high priority vulnerabilities, and delineates mitigation procedures that will be used to address those vulnerabilities at the three MARSEC levels. Form CG-6025 is part of the FSP (Section 18).

It should be pointed out that instructions for completion of the form and a key for the codes to be used on it accompany the actual form.

11.6 Compliance inspections

Instructors should distinguish for trainees the two primary types of USCG facility security inspections. It should be noted that FSOs should expect not less than two inspections each year: one scheduled and one unannounced.

Trainees should become familiar with the checklists that are used by USCG inspectors, which are found in the enclosures to NVIC 03-03, Change 2. They should also learn that in preparation for a scheduled inspection, they should review the FSP, verify that all pertinent documents are in order, and ensure that all drills, equipment tests, etc., have been properly recorded.

If deficiencies are identified during the exam, depending on severity, the outcome may be that the facility is given an opportunity to rectify them within a prescribed period of time. Where more serious problems are discovered, or in cases where deficiencies are not corrected as directed by the Coast Guard, the agency can issue a letter of warning, a notice of violation, impose a civil penalty such as a fine, or suspend operations of the facility completely.

12. Trainee Assessment

12.1 Assessment of knowledge, understanding, proficiency, and skill

Ideally, multiple forms of assessment will take place throughout the course. In this final stage, participants will demonstrate through appropriate assessments their overall mastery of the course material and their ability to correctly apply it. A discussion of assessments is found in Part E of this model course.

Part E: Assessment

Introduction

Trainees in the FSO course must demonstrate their knowledge, understanding, and proficiency in the topics prescribed for the course in order to receive a course completion certificate. Training providers are expected to take great care in ensuring that valid and reliable assessments that accurately measure trainee competence are developed and administered. Ultimately, these assessments should be focused on verifying that the trainee, having completed the course, is capable of applying what has been learned and doing the job of a designated FSO.

Competence-based assessment

The goal of competence-based assessment is to collect evidence that trainees are able to meet specific performance standards and to effectively fulfil a given occupational role. The measurement of knowledge acquisition should occur in connection with job-related performance criteria. Competence-based assessment is intended to show that trainees can perform relative to specified standards, that they can achieve those performance standards consistently, and that they can perform over a range of contexts or conditions.

Key features of a competence-based assessment include:

- a focus on outcomes
- individualized assessment
- no percentage ratings
- no comparison with other candidates
- all standards must be met
- on-going process (further development)
- only “competent” or “not yet competent”[4]

Assessments should take place throughout the course (for example, at the conclusion of each module) as well as at the end of the course, when written and practical exams should be administered.

Assessment methods

The methods selected for a given assessment will depend upon what the trainee is expected to achieve in terms of knowing, comprehending, and applying the course content.

[4] Compton, D. (2011). “Competence-based assessment.” (Unpublished paper).

The methods used can range from simple question-and-answer discussions with trainees (either individually or as a group) to prepared multiple-choice exams requiring the selection of correct or best responses from given alternatives, the correct matching of given items, the supply of short answers, or the generation of more extensive written responses to essay-type questions.

In all of these approaches, careful attention should be paid to question validity and the use of appropriate metrics. Verbal questioning should employ rating sheets and provide for proper recording of results.

Where the course content is aimed at the acquisition of practical skills, the test will involve a practical demonstration by the trainee, making use of appropriate equipment, tools, etc. A systematic approach to evaluation is essential to ensuring maximum objectivity in this kind of assessment. Checklists containing clear performance objectives are an important tool in evaluating demonstration of competence in a practical setting.

The responses requested in a given assessment may involve:

- the recall of facts or information
- the practical demonstration of an attained skill
- the oral or written description of procedures or activities
- the identification and use of data from sketches, drawings, maps, charts, etc.
- the demonstration of correct action in a simulated emergency

Assessment development

The basic steps in developing an assessment include the following:

- Step 1: Specify Assessment Objectives
- Step 2: Determine Assessment Methods
- Step 3: Specify Assessment Conditions
- Step 4: Develop Proficiency Criteria
- Step 5: Prepare Assessment Materials

The competences and learning objectives that are listed in the course will provide a solid foundation for the construction of suitable tests for evaluating trainee progress.

Validity and reliability

An assessment is *valid* when it accurately measures the job-critical knowledge, skills, and abilities required for proficient job performance. An assessment is *reliable* when it consistently obtains the same results across subjects with comparable skills. An assessment will be valid if the conditions of assessment reasonably reflect a representative range of working conditions and requirements. Some questions that should be considered in determining whether or not a valid assessment is being conducted include the following:

- Will the assessment be conducted under realistic working conditions that adequately assess the trainee's abilities to perform his or her duties on the job?

- Will the trainee be required to demonstrate the skills and knowledge that are identified in the assessment as critical to proficiency?
- Will the trainee be required to rely on his or her own skills and knowledge?[5]

Objective testing

The distinguishing feature of objective testing is that the evaluation does not require a judgment by the evaluator. If this question is valid, the response is either right or wrong.

One type of objective test involves supplying an answer, generally a single word, to complete the missing portion of a sentence. Another involves supplying a short answer of two or three words to a question. Such tests are known as “completion tests” and “short answer tests.”

Another form of objective testing consists of “selective response tests” in which the most correct, or “best” response must be selected from given alternatives. Such tests may consist of “matching tests,” in which items contained in two separate lists must be matched; true/false questions; or multiple-choice items.

The most flexible form of objective test is the multiple-choice test, which presents the trainee with a problem and a list of alternative solutions, from which he or she must select the most appropriate answer.

Distracters

The incorrect alternatives in multiple-choice questions are called “distracters,” because their purpose is to distract the uninformed trainee from the correct response. The distracter must be realistic and should be based on misconceptions commonly held, or on mistakes commonly made.

The options “none of the above” or “all of the above” are used in some tests. These can be helpful, but should be used sparingly.

Distracters should distract the uninformed, but they should not take the form of “trick” questions that could mislead the knowledgeable trainee (for example, do not insert “not” into a correct response to make it a distracter).

Scoring

In simple scoring of objective tests one point may be allotted to each correct response and zero for a wrong or omitted response.

The “guess factor” with four alternative responses in a multiple-choice test would be 25%. The determination of a passing score for this type of exam should take this fact into account.

A more sophisticated scoring technique entails awarding one point for a correct response, zero for an omitted response, and minus one for an incorrect response. Where a multiple-choice test involves four alternatives, this means that a totally uninformed guess involves a 25% chance of gaining one point and a 75% chance of losing one point.

[5] USCG R&D Center. (2000). Assessor’s Manual for Conducting Mariner Assessments. USCG: Groton.

Scores can be weighted to reflect the relative importance of questions, or of sections of an evaluation.

Appendix A: Sample Additional Module--Container Facilities

Module Outline

Subject Area

1. Customs and Border Protection (CBP) initiatives
2. World Customs Organization (WCO) initiatives
3. Contraband and human smuggling via cargo and containers
4. Container inspection techniques
5. Container seals and their vulnerabilities
6. Prevention of cargo theft

Learning Objectives

1. Customs and Border Protection (CBP) initiatives
   .1 list the principal CBP programs pertaining to container security and their objectives
2. World Customs Organization (WCO) initiatives
   .1 list the principal WCO programs pertaining to container security and their objectives
3. Contraband and human smuggling via cargo and containers
   .1 explain the use of containers for the illegal transportation of contraband items and people
4. Container inspection techniques
   .1 list the types of container inspection techniques and their application
5. Container seals and their vulnerabilities
   .1 describe the various types of container seals and the techniques that can be used to defeat them
6. Prevention of cargo theft
   .1 summarize key strategies and techniques for the prevention of cargo theft

1. Customs and Border Protection (CBP) initiatives

Instructors should note for students that the Department of Homeland Security's Customs and Border Protection (CBP) has the primary responsibility for U.S. border and cargo security. A number of CBP initiatives further protection of the United States against terrorism, smuggling, and other criminal activities involving the nation's ports and marine transportation system.

Container Security Initiative (CSI)[6]

CSI addresses the threat to border security and global trade posed by the potential for terrorist use of a maritime container to deliver a weapon. CSI proposes a security regime to ensure all containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the United States. CBP has stationed multidisciplinary teams of U.S. officers from both CBP and Immigration and Customs Enforcement (ICE) to work together with our host foreign government counterparts. Their mission is to target and prescreen containers and to develop additional investigative leads related to the terrorist threat to cargo destined to the United States.

The three core elements of CSI are:

- Identify high-risk containers. CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism, based on advance information and strategic intelligence.
- Prescreen and evaluate containers before they are shipped. Containers are screened as early in the supply chain as possible, generally at the port of departure.
- Use technology to prescreen high-risk containers to ensure that screening can be done rapidly without slowing down the movement of trade. This technology includes large-scale X-ray and gamma ray machines and radiation detection devices.

Through CSI, CBP officers work with host customs administrations to establish security criteria for identifying high-risk containers. Those administrations use non-intrusive inspection (NII) and radiation detection technology to screen high-risk containers before they are shipped to U.S. ports.

Announced in January 2002, CSI is now operational at ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America. CBP's 58 operational CSI ports now prescreen over 80 percent of all maritime containerized cargo imported into the United States.

Customs-Trade Partnership Against Terrorism (C-TPAT)[7]

C-TPAT was established in 2001 to help safeguard world trade from terrorists, maintaining the economic health of the U.S. and its neighbors. The partnership develops and adopts measures that add security but do not have a chilling effect on trade.

As of June 2011, more than 10,000 certified partners have been accepted into the program. These include U.S. importers, U.S./Canada highway carriers; U.S./Mexico highway carriers; rail and sea carriers; licensed U.S. Customs brokers; U.S. marine port authority/terminal operators; U.S. freight consolidators; ocean transportation intermediaries and non-operating common carriers; Mexican and Canadian manufacturers; and Mexican long-haul carriers. These 10,000-plus companies account for over 50 percent (by value) of cargo imported into the United States.

---

[6] U.S. Customs and Border Protection. CSI in Brief. http://cbp.gov/xp/cgov/trade/cargo_security/csi/csi_in_brief.xml.

[7] U.S. Customs and Border Protection. C-TPAT Overview. http://cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_program_information/what_is_ctpat/ctpat_overview.ctt/ctpat_overview.pdf

By extending the United States' zone of security to the point of origin, C-TPAT allows for better risk assessment and targeting, freeing CBP to allocate resources to inspect more questionable shipments. The partnership establishes clear supply chain security criteria for members to meet and in return provides incentives and benefits such as expedited processing. When they join the anti-terror partnership, companies sign an agreement to work with CBP to protect the supply chain, identify security gaps, and implement specific security measures and best practices. Additionally, partners provide CBP with a security profile outlining the specific security measures the company has in place. Applicants must address a broad range of security topics and present security profiles that list action plans to align security throughout their supply chains. C-TPAT members are considered low-risk and are therefore less likely to be examined. This designation is based on a company's past compliance history, security profile, and the validation of a sample international supply chain.

Carrier Initiative Program (CIP)[8]

CBP provides anti-drug smuggling training to air, sea, and land carriers. This training is part of the CBP Carrier Initiative and Super Carrier Initiative Programs under which CBP and transportation companies cooperate to prevent commercial conveyances from being utilized to smuggle narcotics.

Carrier Initiative training is directed at employees of air, sea and land commercial carriers. Those carriers with route systems that are high risk for drug smuggling voluntarily sign agreements with CBP. The carriers agree to exercise the highest degree of care and diligence in securing their facilities and conveyances, while CBP agrees to conduct site surveys and provide appropriate training and recommendations for improving security. The degree of a carrier's compliance with the agreement may become a mitigating factor in the assessment of a penalty if narcotics are found on board a conveyance. The Super Carrier Initiative Program is for those carriers that face an extraordinarily high risk from drug traffickers. CBP and various carriers have signed over 3,800 Carrier Initiative Agreements and 27 Super Carrier Agreements.

CBP offers two training programs: a two-day anti-drug smuggling seminar for senior level managers and a one-day anti-drug smuggling seminar for mid-level managers, supervisors and front-line personnel.

Topics included in the one-day seminar are:

- search techniques
- risk assessments
- concealment techniques
- document review
- physical and procedural security
- personnel hiring
- drug source countries
- drug characteristics
- internal smuggling conspiracies

In addition to the above topics, the two-day seminar provides an in-depth review of the legal issues concerning carrier liability and deals with penalty and mitigation procedures.

[8] U.S. Customs and Border Protection. Carrier Initiative Program (CIP). http://www.cbp.gov/xp/cgov/border_security/international_operations/partnerships/cip.xml

The overall goals of these programs and their training component are to encourage commercial carriers to share with CBP the burden of stopping the flow of illicit drugs; to deter smugglers from using commercial carriers to smuggle drugs; and to provide carriers with the incentive to improve their security and their drug smuggling awareness.

Business Alliance for Secure Commerce (BASC)[9]

The Business Alliance for Secure Commerce (BASC) is a private sector led and controlled coalition that has been supported by CBP since its creation in 1996. BASC is an international business alliance created to promote supply chain security in cooperation with government agencies and international organizations.

BASC was created to address the problem of concealing contraband in commercial trade. As a voluntary program for businesses, with no government-imposed mandates, corporate participants are expected to follow BASC's security standards which are designed to significantly improve their security practices and in the process deter contraband smugglers and terrorists from using their companies to introduce contraband and implements of terror in legitimate shipments.

The BASC program examines the entire process of manufacturing and shipping of merchandise from foreign countries to the United States, emphasizing the creation of a more security-conscious environment throughout the supply chain. The BASC currently has over 2,500 companies that have been certified by the organization. It operates in 12 countries of Latin America and the Caribbean: Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Haiti, Mexico, Panama, Peru, the Dominican Republic, Uruguay, and Venezuela.

Americas Counter Smuggling Initiative (ACSI)[10]

The Americas Counter Smuggling Initiative (ACSI) is a priority undertaking by CBP under C-TPAT that is designed to counter the smuggling of drugs and the possible introduction of implements of terror in commercial cargo and conveyances. ACSI focuses on each aspect of the commercial transportation process and offer a more comprehensive approach to dealing with this problem.

Since February 1998, under the auspices of ACSI, CBP officers have been detailed overseas to assist exporters, carriers, manufacturers and other businesses. These officers aid in the development and implementation of security programs and initiatives to safeguard legitimate trade from being used to smuggle drugs. ACSI teams consists CBP officers who provide border protection expertise, provide security training, speak at seminars, and perform limited site surveys at manufacturing plants and port facilities. ACSI teams are travelling to work with BASC companies in Colombia, Costa Rica, Ecuador, Mexico, Panama, Peru, Venezuela, Jamaica and the Dominican Republic. Additionally, the teams work with foreign governments and law enforcement agencies to help improve their efforts against contraband smugglers and in their development of industry partnerships.

---

[9] U.S. Customs and Border Protection. Business Alliance for Secure Commerce (BASC) / World BASC Organization (WBO). http://www.cbp.gov/xp/cgov/border_security/international_operations/partnerships/basc.xml

[10] U.S. Customs and Border Protection. Americas Counter Smuggling Initiative (ACSI). http://www.cbp.gov/xp/cgov/border_security/international_operations/partnerships/acsi.xml

24-Hour and Importer Security Filing ("10+2") Rules

CBP requires advance information on shipments from overseas to be submitted electronically before they arrive in the United States. The Trade Act of 2002, as operationalized through regulation commonly known as the "24-Hour Rule," requires ocean carriers and NVOCCs (Non-Vessel Operating Common Carriers) to provide CBP with detailed descriptions of the contents of containers bound for the United States not less than 24 hours before the container is loaded at the foreign port. The Importer Security Filing and Additional Carrier Requirements rule (Security Filing "10+2") mandates that importers provide ten specific items of information concerning import cargoes to CBP; carriers are required to transmit the stow plan of the vessel and Container Status Messages, in addition to the advance information required by the 24-Hour Rule.[11]

2. World Customs Organization (WCO) initiatives

The World Customs Organization (WCO) is the only intergovernmental organization exclusively focused on Customs matters. With its worldwide membership, the WCO is now recognized as the voice of the global Customs community. It is particularly noted for its work in areas covering the development of global standards, the simplification and harmonization of Customs procedures, trade supply chain security, the facilitation of international trade, the enhancement of Customs enforcement and compliance activities, anti-counterfeiting and anti-piracy initiatives, public-private partnerships, integrity promotion, and sustainable global Customs capacity building programs. The WCO also maintains the international Harmonized System goods nomenclature, and administers the technical aspects of the WTO Agreements on Customs Valuation and Rules of Origin.[12]

The WCO has adopted a series of measures to be used by its Members in securing the international trade supply chain while facilitating the flow of legitimate trade and implementing their national requirements. The measures were made in response to international concerns that the trade supply chain could be used for the transport of weapons of mass destruction.

The measures approved by the Council included:

- A new international convention and commentary on Mutual Administrative Assistance in Customs Matters – Johannesburg Convention
- The WCO Data Model and a list of essential data elements required for the identification of high risk consignments
- International Customs guidelines on advance cargo information, subject to further work being undertaken on industry specific guidelines
- Guidelines for the development of national laws for the collection and transmission of Customs information
- High level guidelines for co-operative arrangements between WCO Members and the private sector to increase supply chain security
- Enhancements of the WCO's information and intelligence strategy including the operation of its global Regional Intelligence Liaison Offices network

[11] CBP. (2008, November 25). Importer Security Filing and Additional Carrier Requirements. Interim Final Rule. Federal Register / Vol. 73, No. 228. 71730.
[12] World Customs Organization. About Us. http://www.wcoomd.org/home_about_us.htm

- A new internet-based Databank on advanced technology to enable WCO Members to identify products and services for the detection of illegal consignments and contraband.[13]

3. Contraband and human smuggling via cargo and containers

Students should be familiarized with the vast array of creative methods used by stowaways, terrorists, and criminals to utilize cargo and containers for the illicit transportation of contraband and people. Articles of contraband, such as drugs, are frequently hidden inside concrete blocks, fence posts, batteries, ceramic products, vehicles, and many other items of cargo. Contraband is also commonly concealed inside machinery that is difficult to disassemble for inspection. Containers are also often used to smuggle contraband through such techniques as the construction of secret compartments, fabrication of false walls, and the dismantling and reassembly of container components.[14]

The illegal and covert transportation of migrants, terrorists, and other person in cargo and containers occurs with unknown frequency, given the fact that many such incidents surely go undetected. Beyond utilization of the myriad hiding places aboard ships, human smuggling occurs via cargo and containers through such techniques as concealment inside cargo pallets, boxes, empty containers, and vehicles.

4. Container inspection techniques

Course participants should be acquainted with the tools and techniques that are employed to detect attempts to smuggle people and illegal articles using cargo containers.

The seven primary areas of focus for container inspection are:[15]

- Front wall
- Left wall
- Right wall
- Floor
- Roof
- Undercarriage and supports
- Doors

5. Container seals and their vulnerabilities[16]

Trainees should understand the use of various types of container seals and the ways in which they can be defeated. Seals play a crucial role in ensuring the integrity of containers and in facilitating trade and Customs processes. Both mechanical cargo seals and electronic seals ("e-Seals") help to deter pilferage, smuggling, and sabotage of cargo within containers and trailers. If either type of seal is found to be broken or if its identification (ID) number is different from the one on the cargo document, this is an indication that the container or trailer door might have

[13] World Customs Organization. Enforcement and Compliance - Responsibilities > Global Supply Chain Security. http://www.wcoomd.org/home_wco_topics_epglobalsupplychainfacilitationandsecurity.htm

[14] McNicholas, M. (2008.) *Maritime Security: An Introduction*. Butterworth-Heinemann, Burlington. 197-213.

[15] McNicholas, M. (2008.) *Maritime Security: An Introduction*. Butterworth-Heinemann, Burlington. 349.

[16] Adapted from: The International Bank for Reconstruction and Development / The World Bank. (2009). *Supply Chain Security Guide.* Washington, DC.

been opened by an unauthorized person at some point in the transportation route. The ID number on the seal should be recorded at each handoff in the chain of custody to provide information about when and where the container or trailer was handed over and the status of the seal at that time.

Instructors should point out that the party responsible for stuffing and sealing the container is the first, and most important, link in a “secure” container transport chain. It should be emphasized that even high-security mechanical seals are only as good as the procedures in place to affix, monitor and document them at each transfer of responsibility.

The critical importance of proper sealing protocols such as the following should be discussed:

- Purchasing/sourcing and shipping procedures for seals
- Training in seal use and verification
- Tracking of seal inventories and safe storage/release procedures
- Correct application of seals
- Recording seal numbers
- Managing and transmitting seal numbers
- Recording seal operations and identification of people involved and time and date
- Recording seal anomalies
- End-of-use and end-of-life disposal of seals.

Without proper sealing and checking protocols, the use of seals can be counter-productive as they can instill a false sense of security as to the status of the container handle/door. In theory, security seals should prove effective in detecting any attempt to tamper with the container.

In practice, simple security seals are relatively easy to defeat. The reasons include the ease with which seals can be cut, the possible lack of proper seal documentation, the possibility of poor security management in the container transport chain and the relative ease of replicating certain seals and their numbers. As with simple indicative seals, verifying the seal is both a manual and time-consuming process and thus many seals are only summarily checked, if checked at all, while in transit. It is important to note that thieves have devised ways to bypass the handle or the container doors entirely when gaining entry to the container. Exterior panels can be removed and reinstalled by skilled criminals, leaving little or no evidence of the breach.

The high security seal is one that is made of material, such as metal or metal cable, with the intent to delay intrusion. High security seals generally must be removed with quality bolt cutters or cable cutters. They require inspection to indicate whether tampering has occurred or entry has been attempted. All containers in transit to the United States are now required to be sealed with a seal meeting the International Organization for Standardization Publicly Available Specification 17712 (ISO/PAS 17712) standard for sealing containers. Prospective FSOs should be aware that all containers arriving by vessel at any port of entry in the United States are required to be sealed with a seal meeting the ISO/PAS 17712 standard.

1. Prevention of cargo theft

Trainees should be aware that cargo theft is a multi-billion dollar problem in the United States. According to a recent report, overall cargo theft rates have increased every year since 2006. The growth rate of cargo theft has now begun to level off somewhat as shippers and their transportation providers work to strengthen the security of supply chains handling high-value

cargo. As a result of these efforts, the average loss value per stolen load decreased by 17 percent from 2009 to 2010.[17]

Course participants should be advised that most cargo theft takes place in terminals, consolidation/deconsolidation facilities, and similar locations. The prevalence of cargo containerization also means that where in earlier eras individual items of break-bulk cargo might have been pilfered, today entire containers are stolen, often as part of organized crime conspiracies.

Instructors should discuss strategies and tactics that can be used to reduce cargo theft, such as the following recommendations:[18]

1. Thoroughly screen prospective employees. Some cargo security experts maintain that a high percentage of cargo thefts involve inside information or complicity.
2. Carefully select transportation partners and intermediaries. Remember that these companies have care, custody and control of goods once they leave your premises until they reach their destination.
3. Establish a security culture within your company. Provide security training for employees, and educate truck drivers in hijack awareness and prevention.
4. Factor in security when determining shipment routing. Cargo thieves often "case" known shipping points (plants, warehouses and distribution centers) and follow trucks as they depart, waiting for the drivers to stop so that they can pounce on the loads. Drivers should not be allowed to stop in the "red zone" (the first 200 miles/4 hours from their starting point) as well as known hot spots.
5. Incorporate counter surveillance into the duties of security guards, and have guards patrol away from perimeters.
6. Take advantage of technology. Vehicle and shipment tracking, vehicle immobilization and advanced, high-technology security seals are now available at lower cost.
7. Conduct periodic security audits. Operations and personnel change, and criminals are always harvesting fresh ideas and modifying previous techniques.

[17] Freightwatch. (2011, 27 April). “US Cargo Theft: A Five-Year Review.” http://www.asisonline.org/toolkit/freightwatch.pdf

[18] “Rethinking Security and Logistics Can Help Reduce Risk of Cargo Theft.” http://www.chubb.com/corporate/chubb8937.html