U.S. Department of Transportation
Maritime Administration

Vessel Security Officer

Model Course MTSA 08-01

Prepared by

THE UNITED STATES MERCHANT MARINE ACADEMY

30 April 2008

Foreword

This course is one of a series originally developed by the U.S. Maritime Administration (MARAD) in fulfillment of its charge under the Maritime Transportation Security Act of 2002 (MTSA 2002). Section 109 of the Act 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 by the Maritime Administrator to the U.S. Merchant Marine Academy for execution.

Through a collaborative effort with industry and other government agencies, the Academy created seven model course frameworks in response to the training needs identified by the Congress and articulated in the MTSA 2002. These model course frameworks, and a discussion of key issues related to maritime security education and training, are contained in MARAD's Report to Congress titled "*Maritime Transportation Security Act of 2002: Section 109 Implementation."*

The MTSA project led to the creation by the U.S. Merchant Marine Academy, in a joint effort with the United States Coast Guard and the Directorate General of Shipping, Government of India, of three model courses for the International Maritime Organization (IMO). The Ship Security Officer, Company Security Officer, and Port Facility Security Officer courses were published by the IMO in September 2003 and are now the global benchmarks for maritime security training.

In a style similar to that of the IMO model courses, the course that follows provides a blueprint for the training of Vessel Security Officers. This course will serve as the reference for course approval and certification required under U.S. Coast Guard regulation.

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

Sean T. Connaughton
Maritime Administrator

Contents

Introduction

This model course is intended as guidance upon which education and training providers can base instruction in maritime 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 standards of competence and the acquisition of specific understanding through education and training. In addition, expert advice and public comment have been solicited and obtained through a focused public outreach effort.

This model course constitutes a base-level curriculum for maritime security education and training that includes the competences listed in the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), 1978, as amended, those subjects listed in MTSA Sec. 109 (b)(2), 33 CFR Chapter I, Subchapter H, and in the SAFE Port Act of 2006 Sec. 113 (b)(4)(A)-(J) In addition to delineating the security duties and responsibilities of personnel and the training necessary to meet the requirements, the curriculum suggests resources that can be employed in delivery of the material. These resources include reports, regulations, conventions, books, videotapes, and other adjuncts to education and training that will assist instructors in conducting the training envisioned in pertinent regulation and guidance.

This course for Vessel Security Officer is based on the International Maritime Organization's Model Course for Ship Security Officer. The present course has been revised and updated for U.S. domestic purposes to reflect the mandatory training requirements in 33 CFR Chapter I, Subchapter H, the latest requirements of the SAFE Port Act of 2006 and the TWIC program, and other recent developments.

Part A: Course Framework

■ Scope

This model course is intended to provide the knowledge required for personnel who are assigned responsibilities as Vessel Security Officer (VSO) to perform their duties in accordance with the requirements of the Maritime Transportation Security Act of 2002, Chapter XI-2 of SOLAS 74 as amended, the IMO ISPS Code, and U.S. Coast Guard regulations contained in 33 CFR Chapter I Subchapter H. The course aim is also to meet the mandatory minimum requirements for knowledge, understanding and proficiency in Table A-VI/5 of the STCW Code and the mandatory training requirements in 33 CFR Part 104.

■ Objective

This syllabus covers the requirements of the STCW Code Chapter VI, Section A-VI/5. Those who successfully complete this course should be able to undertake the duties and responsibilities of a designated Vessel Security Officer as defined in 33 CFR Part 104, which include, but are not limited to:

1. Regularly inspecting the vessel to ensure that security measures are maintained;

2. Ensuring maintenance and supervision of the implementation of the VSP, and any amendments to the VSP;

3. Ensuring the coordination and handling of cargo and vessel stores and bunkers in compliance with this part;

4. Proposing modifications to the VSP to the Company Security Officer (CSO);

5. Ensuring that any problems identified during audits or inspections are reported to the CSO, and promptly implement any corrective actions;

6. Ensuring security awareness and vigilance on board the vessel;

7. Ensuring adequate security training for vessel personnel;

8. Ensuring the reporting and recording of all security incidents;

9. Ensuring the coordinated implementation of the VSP with the CSO and the relevant Facility Security Officer, when applicable;

10. Ensuring security equipment is properly operated, tested, calibrated, and maintained;

11. Ensuring consistency between security requirements and the proper treatment of vessel personnel affected by those requirements; and

12. Ensuring TWIC programs are in place and implemented appropriately.

Entry standards

It is assumed that those attending this course are U.S. Coast Guard credentialed mariners who are employed (or are to be employed) by a vessel owner or operator and who are likely to be designated as Vessel Security Officer (VSO). 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 a VSO. Training providers are responsible for verifying that these conditions are met before accepting candidates for training.

Course completion certificate

A course completion certificate should be issued upon successful completion of the course and assessments, certifying that the holder has successfully completed "Vessel Security Officer" training that meets the requirements in Table A-VI/5 of the STCW Code and the mandatory training requirements in 33 CFR Part 104.

Course delivery

The objectives of this course may be achieved through various methods, including classroom training, in-service training, distance learning, computer-based training or combinations of these methods.

Course intake limitations

The maximum number of trainees in the course should be determined based on the facilities and equipment available, bearing in mind the aims and objectives of this course.

Instructor Qualifications

The instructor in charge of the course shall have had training and/or acceptable equivalent practical experience in the subject matter of this course, including knowledge of vessel, facility, and port operations, maritime security matters, and the requirements of the Maritime Transportation Security Act of 2002, Chapter XI-2 of SOLAS 74 as amended, the IMO ISPS Code, and relevant U.S. Coast Guard regulations.

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

Teaching facilities and equipment

An ordinary classroom or similar meeting room with a blackboard or equivalent is sufficient for the lectures. In addition, when making use of audiovisual materials, it should be ensured that appropriate equipment is available. Finally, the use of maritime environments (vessels, facilities, or mock-ups) for certain segments of the course may enhance the overall effectiveness of this training.

Teaching aids

Model Course MTSA 08-01, Vessel Security Officer

Audiovisual aids: videocassette player, TV, slide projector, overhead projector, etc.

Photographs, models, or other representations of vessels, facilities, devices, etc., to illustrate operational elements and security vulnerabilities.

Video cassette(s)

Distance learning package(s)

Training reference documents

■ Training references

Coast Guard, Department of Homeland Security. (2003, 22 October). *33 CFR (Navigation and Navigable Waters), Chapter I, Subchapter H—Maritime Security, Parts 101, 103, 104.*

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. (2003, 13 January). "Recommended Security Guidelines for Facilities." *Navigation and Vessel Inspection Circular (NVIC) No. 11-02.*

Commandant, United States Coast Guard. (2002, April). "Security for Passenger Vessels and Passenger Terminals." *Navigation and Vessel Inspection Circular (NVIC) No. 4-02.*

Commandant, United States Coast Guard. (2002, 21 October). "Security Guidelines for Vessels." *Navigation and Vessel Inspection Circular (NVIC) No. 10-02.*

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.

Hawkes, K. G. (1989). *Maritime Security.* Centreville: Cornell Maritime Press.

International Chamber of Shipping. (2003*). Maritime Security: Guidance for Ship Operators on the IMO International Ship and Port Facility Security Code.* London: ICS.

International Chamber of Shipping. (2003). *Model Ship Security Plan.* London: ICS.

International Chamber of Shipping/International Shipping Federation. (2004). *Pirates and Armed Robbers: Guidelines on Prevention for Masters and Ship Security Officers.* (4th ed.). London: Marisec Publications.

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. (2003). *Model Course 3.19: Ship Security Officer, 2003 edition*. London: IMO. (IMO-T319E).

International Maritime Organization. (1986). *MSC/Circ.443--Measures to prevent unlawful acts against passengers and crews on board ships.*

International Maritime Organization. (1993). *Res.A.738(18)--Measures to prevent* and suppress piracy and armed robbery against *ships.*

International Maritime Organization. (2001). *STCW Convention, 2006 Amendments*. London: IMO.

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.

United States Coast Guard. *Risk-based Decision Making Guidelines.* (3rd ed.). http://www.uscg.mil/hq/g-m/risk/e-guidelines/rbdm.htm

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

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

Viollis, P., et al. (2002). *Jane's Workplace Security Handbook.* (1st ed.). Alexandria: Jane's Information Group.

Part B: Course Outline

Subject Area		Hours
1	**Introduction**	1.5
1.1	Course overview	
1.2	Competences to be achieved	
1.3	Historical perspective	
1.4	Current security threats and patterns	
1.5	Vessel and port operations and conditions	
2	**Maritime Security Policy**	1.6
2.1	Relevant international conventions, codes, and recommendations	
2.2	Relevant government legislation, regulations, and guidance	
2.3	Definitions	
2.4	Legal implications of action or non-action by security personnel	
2.5	Handling sensitive security-related information and communications	
3	**Security Responsibilities**	2.3
3.1	Contracting governments	
3.2	The company	
3.3	The vessel	
3.4	The Master	
3.5	The facility	
3.6	Vessel Security Officer	
3.7	Company Security Officer	
3.8	Facility Security Officer	
3.9	Vessel personnel with specific security duties	
3.10	Facility personnel with specific security duties	
3.11	Other personnel	
4	**Vessel Security Assessment**	1.7
4.1	Risk assessment methodology	
4.2	Assessment tools	

Subject Area			Hours
	4.3	On-scene security surveys	
	4.4	Security assessment documentation	
5	**Security Equipment**		1.0
	5.1	Security equipment and systems	
	5.2	Operational limitations of security equipment and systems	
	5.3	Testing, calibration and maintenance of security equipment and systems	
6	**Vessel Security Plan**		1.6
	6.1	Purpose of the Vessel Security Plan	
	6.2	Contents of the Vessel Security Plan	
	6.3	Confidentiality issues	
	6.4	Implementation of the Vessel Security Plan	
	6.5	Maintenance and modification of the Vessel Security Plan	
7	**Threat Identification, Recognition, and Response**		2.9
	7.1	Recognition and detection of dangerous substances and devices	
	7.2	Methods of screening, physical searches, and non-intrusive inspections	
	7.3	Implementing and coordinating searches	
	7.4	Recognition, on a non-discriminatory basis, of persons posing potential security risks	
	7.5	Techniques used to circumvent security measures	
	7.6	Crowd management and control techniques	
8	**Vessel Security Actions**		2.7
	8.1	Actions required by different security levels	
	8.2	Maintaining security of the vessel-to-port and vessel-to-facility interfaces	
	8.3	Usage of the Declaration of Security	
	8.4	Implementation of security procedures	
	8.5	Access control	

Subject Area		Hours
9	**Emergency Preparedness, Drills, and Exercises**	1.2
9.1	Contingency planning	
9.2	Security drills and exercises	
9.3	Assessment of security drills and exercises	
10	**Security Administration**	1.0
10.1	Documentation and records	
10.2	Reporting security incidents	
10.3	Monitoring and control	
10.4	Security audits and inspections	
10.5	Reporting nonconformities	
11	**Security Training**	0.5
11.1	Training requirements	
	Total:	18.0

Part C: Detailed Teaching Syllabus

■ Competences

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

1. Maintaining and supervising the implementation of a Vessel Security Plan;

2. Assessing security risk, threat, and vulnerability;

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

4. Ensuring that security equipment and systems, if any, 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 what the trainee should be able to do to demonstrate that knowledge has been transferred. All objectives are understood to be prefixed by the words, "The expected learning outcome is that the trainee ....."

1. Introduction (1.5 hours)

1.1. Course overview

.1 describes the topics and emphasis of the course

1.2. Competences to be achieved

.1 describes the competences that will be achieved through completion of the course

1.3. Historical perspective

.1 describes representative incidents involving criminal activity in the maritime environment

.2 summarizes incident statistics and discusses underlying motivation and results

1.4. Current security threats and patterns

.1 identifies threats to the Marine Transportation System, such as:

- piracy and armed attacks
- terrorism
- contraband smuggling
- stowaways and refugees
- cargo theft

- collateral damage

1.5. Vessel and port operations and conditions

.1 characterizes the intermodal nature of transportation and the interfaces between vessels and other modes

2. Maritime Security Policy (1.6 hours)

2.1. Relevant international conventions, codes, and recommendations

.1 lists previous efforts of the IMO toward maritime security, such as MSC/Circ.443, SUA Act, etc.

.2 summarizes the amendments to SOLAS Chapter XI and the contents of the ISPS Code

2.2. Relevant U.S. government legislation, regulations, and guidance

.1 states the requirements of relevant legislation, regulations, and guidance

2.3. Definitions

.1 defines

- Breach of security
- Company
- Company Security Officer
- Contracting Government
- Declaration of Security
- Drill
- Escorting
- Exercise
- Facility
- Facility Security Assessment
- Facility Security Officer
- Facility Security Plan
- Infrastructure
- International voyage
- Maritime Security Directive
- Maritime Security Level
- Owner or operator
- Restricted area
- Screening
- Secure area
- Security sweep
- Security system
- Sensitive Security Information
- Survey
- Transportation security incident
- TWIC program
- Unescorted access
- Vessel-to-facility interface

- Vessel-to-port interface
- Vessel-to-vessel activity
- Vessel Security Assessment
- Vessel Security Plan
- Vessel Security Officer
- Vessel personnel with security duties
- Vessel personnel without security duties

2.4. Legal implications of action or non-action by security personnel

.1 identifies the legal limits of authority and the obligations of personnel with security duties including those arising from the TWIC program

2.5. Handling sensitive security-related information and communications

.1 defines security-sensitive information and the importance of keeping it confidential

3. **Security Responsibilities** (2.3 hours)

3.1. Contracting governments

.1 describes the responsibilities of contracting governments with respect to SOLAS Chapter XI-2 and the ISPS Code

3.2. The company

.1 describes the responsibilities of the company with respect to:

- ensuring that the master has documents on board relating to the crewing of the vessel and its employment
- ensuring that the Vessel Security Plan contains a clear statement emphasizing the master's authority
- designating a Company Security Officer and a Vessel Security officer and ensuring that they are given the necessary support to fulfil their duties and responsibilities
- implementation of the TWIC access control

3.3. The vessel

.1 states that the vessel shall comply with the requirements of the Vessel Security Plan as per the security level set

3.4. The Master

.1 describes the authority, duties, and responsibilities of the Master pertaining to security

3.5. The facility

.1 states that facilities shall comply with the relevant requirements of 33 CFR Subchapter H, Chapter XI-2 of SOLAS, and the ISPS Code

.2 states that the facility shall act upon the security levels set by the Administration within whose territory it is located

3.6. Vessel Security Officer

.1 lists the duties and responsibilities of the Vessel Security Officer

3.7. Company Security Officer

.1 describes that the person designated as Company Security Officer may act as Company Security Officer for one or more vessels provided that it is clearly identified for which vessels he/she is responsible

.2 indicates that the company may designate several persons as Company Security Officer provided that it is clearly identified for which vessels each is responsible

.3 lists the duties and responsibilities of the Company Security Officer

3.8. Facility Security Officer

.1 states that a Facility Security Officer shall be designated for each facility

.2 states that a person may be designated as the Facility Security Officer for one or more port facilities

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

3.9. Vessel personnel with specific security duties

.1 states that members of the vessel's crew may be assigned security duties in support of the Vessel Security Plan

3.10. Facility personnel with specific security duties

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

3.11. Other personnel

.1 states that other vessel and facility personnel may have a role in the enhancement of maritime security

.2 states that personnel other than vessel or facility personnel may have a role in the enhancement of maritime security

4. Vessel Security Assessment (1.7 hours)

4.1. Risk assessment methodology

.1 states the basic principles of risk assessment in day-to-day operations

4.2. Assessment tools

.1 discusses the use of checklists in conducting security assessments

4.3. On-scene security surveys

.1 lists the preparations required prior to an on-scene survey

.2 lists the procedures and measures and operations to be evaluated during an on-scene survey

.3 discusses the security aspects of vessel layout

.4 divides the survey into the following sections:

- Physical security
- Structural integrity
- Personnel protection systems
- Procedural policies
- Radio and telecommunication systems, including computer systems and networks
- Other areas including those covered by the TWIC program

.5 discusses the importance and elements of physical security aboard ship

.6 describes the significance of structural integrity for vessels and other structures

.7 identifies other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations aboard a vessel or within a facility

.8 discusses the identification of vulnerabilities in the above areas and the preparation of countermeasures to address them

.9 states the role of proper procedures in preventing and mitigating security incidents

.10 states the importance of having in place emergency plans to deal with contingencies

.11 explains and demonstrates how to carry out a security assessment with new measures in place and checks if further mitigating measures are required

4.4. Security assessment documentation

.1 describes proper form and practice for recording day-to-day security assessment results

5. Security Equipment (1.0 hour)

5.1. Security equipment and systems

.1 lists the various types of security equipment and systems that can be used aboard vessels and in facilities

5.2. Operational limitations of security equipment and systems

.1 explains the limitations of individual items of equipment and security systems

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

.1 describes the testing, calibration and maintenance requirements for the above security equipment and systems

6. Vessel Security Plan (1.6 hours)

6.1. Purpose of the Vessel Security Plan

.1 states that each U.S-flag vessel shall carry a Vessel Security Plan approved by the U.S. Coast Guard

.2 explains that the Vessel Security Plan addresses the security measures that should be taken at each maritime security level

6.2. Contents of the Vessel Security Plan

.1 lists the required elements of a Vessel Security Plan

.2 states that the Vessel Security Plan shall establish procedures for the performance of vessel security duties.

6.3. Confidentiality issues

.1 states that the Vessel Security Plan is confidential

.2 states that the Vessel Security Plan is not generally subject to inspection by Port State Control

.3 describes the circumstances under which certain sections of the plan may be shown to Port State Control authorities

6.4. Implementation of the Vessel Security Plan

.1 explains procedures to be employed in implementing the Vessel Security Plan

.2 explains the requirement to coordinate implementation of the Vessel Security Plan with the Company Security Officer and the Facility Security Officer

.3 discusses the importance of giving due regard to the effect that security measures may have on vessel personnel who may remain on board the vessel for long periods

6.5. Maintenance and modification of the Vessel Security Plan

.1 explains mechanisms for ensuring the continuing effectiveness and updating of the Vessel Security Plan

.2 explains the procedures for implementing any corrective actions

.3 states that amendments to the plan shall not be implemented unless approved by the U.S. Coast Guard

7. Threat Identification, Recognition, and Response (2.9 hours)

7.1. Recognition and detection of dangerous substances and devices

.1 describes the various types of dangerous substances and devices, the damage they can cause, and their appearance

7.2. Methods of screening, physical searches, and non-intrusive inspections

.1 demonstrates how to carry out screening, physical searches, and non-intrusive inspections

.2 describes in brief the use of metal detectors, X-ray machines, and Ion scan machines

7.3. Implementing and coordinating searches

.1 describes how important it is to plan a search and practice carrying out searches as a drill.

.2 explains how to plan a search using a system of check cards

.3 describes the equipment the search team should carry for conducting a search

.4 describes the procedures to be followed for an efficient search

.5 describes the various places of concealment on board a vessel

7.4. Recognition, on a non-discriminatory basis, of persons posing potential security risks

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

.2 states the importance of observation in recognizing such persons

7.5. Techniques used to circumvent security measures

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

7.6. Crowd management and control techniques

.1 explains the basic psychology of a crowd in a crisis situation

.2 states the importance of clear communication with crew and passengers during an emergency

8. Vessel Security Actions (2.7 hours)

8.1. Actions required by different security levels

.1 states the three security levels and the actions required for each level.

.2 lists processes and procedures for crisis management and communications with emergency response providers.

.3 identifies the appropriate implementation of procedures outlined in the National Incident Management System (NIMS) and the National Response Framework (NRF).

8.2. Maintaining security of the vessel-to-port and vessel-to-facility interfaces

.1 lists the reporting requirements for the vessel prior to entering a facility or port

.2 states the importance of knowing established procedures for interfacing with ports, facilities, and other vessels at all MARSEC levels

8.3. Usage of the Declaration of Security

.1 explains the Declaration of Security and what it addresses.

.2 states who determines when it should be completed

.3 lists the situations in which the vessel can request that the Declaration of Security be completed.

.4 states who is required to complete it

8.4. Implementation of security procedures

.1 states the requirements for the Vessel Security Officer to carry out regular security inspections

.2 lists the security measures and procedures at the three security levels required to:

- ensure the performance of all vessel security duties
- control access to the vessel
- control the embarkation of persons and their effects
- monitor restricted and secure areas to ensure only authorized persons have access and that escorts are provided as needed
- monitor deck areas and areas surrounding the vessel
- coordinate the security aspects of the handling of cargo
- maintain security during delivery of vessel stores and bunkers
- ensure that security communication is readily available
- ensure that procedures for security incident response are in place

8.5. Access control

.1 states that the usual requirements for access control can be found in the Vessel Security Plan

.2 states that enhanced access control measures may be required by the TWIC program

.3 lists the TWIC program requirements for escorts in secure areas and the requirements for checking for personal identification including inspection of credentials

9. Emergency Preparedness, Drills, and Exercises (1.2 hour)

9.1. Contingency planning

.1 discusses action to take in case of a breach of security

.2 discusses contingency plans for:

.1 hijacking

.2 bomb threat

.3 unidentified objects / explosives on vessel

.4 damage to / destruction of facility

.5 piracy and other depredations

.6 stowaways

.7 violations of TWIC program requirements

.8 other emergencies

9.2. Security drills and exercises

.1 states the requirements for conducting drills and exercises

9.3. Assessment of security drills and exercises

.1 states the purpose of carrying out an assessment at the end of each drill

10. Security Administration (1.0 hour)

10.1. Documentation and records

.1 states the documents that shall be available on board at all times

.2 describes the International Ship Security Certificate, its validity and verification requirements

.3 states the requirements of the Continuous Synopsis Record and what it shall contain

.4 states the activities for which records shall be kept on board and the duration for which they should be retained.

10.2. Reporting security incidents

.1 states the reporting requirements in case of a security incident or a breach of security including TWIC program violations

10.3. Monitoring and control

.1 states the necessity for the Company Security Officer and the Vessel Security Officer to regularly review and update the Vessel Security Plan and the implicit responsibility of the master in this regard.

10.4. Security audits and inspections

.1 states the requirements for carrying out internal audits and inspections

10.5. Reporting nonconformities

.1 states the requirements for reporting nonconformities and deficiencies identified during internal audits, periodic reviews, and security inspections

11. Security Training (0.5 hour)

11.1. Training requirements

.1 Explains which personnel must receive training and in what subjects they must be trained

.2 Explains the requirement for enhancing security awareness and vigilance onboard

Total: 18.0 hours

Part D: Instructor Manual

The instructor manual provides guidance on the material that is to be presented during the Vessel Security Officer course. This manual reflects the views of the course developers with respect to methodology and organization as well as what they consider relevant and important in light of their experience as instructors. Although the guidance given should be of value initially, each instructor should develop his or her own methods and ideas, recognize and refine what is successful, and discard that which does not work satisfactorily.

The material has been arranged under the following 11 main headings:

1 Introduction
2 Maritime Security Policy
3 Security Responsibilities
4 Vessel Security Assessment
5 Security Equipment
6 Vessel Security Plan
7 Threat Identification, Recognition, and Response
8 Vessel Security Actions
9 Emergency Preparedness, Drills, and Exercises
10 Security Administration
11 Security Training

The detailed teaching syllabus must be studied carefully and, where appropriate, lesson plans or lecture notes should be compiled. The course outline and timetable provide guidance on the time allocation for each topic; however, it should be emphasized that the listed duration of each section represents the minimum time required to convey the specified material.

Preparation and planning are the most important criteria in effectively presenting this course. Availability and proper use of course materials is also essential for maximum efficacy in conveying the subject to trainees. The capabilities and limitations of the facilities in use may dictate that the learning objectives be adjusted but it is suggested that this be kept to a minimum.

Where possible, lectures should be supported by practical demonstrations, table-top exercises, written course materials, videos, and other media that allow the trainee to embrace the material more fully. It will be necessary to prepare material for use with overhead projectors or for distribution to trainees as handouts.

Guidance Notes

1. Introduction

1.1. Course overview

The starting point of instruction should be a brief statement of the purpose of the course, a short review of the timeline, an introduction of the instructor(s) and participants, determination of knowledge and experience levels, and a brief description of the teaching facility.

1.2. Competences to be achieved

The aim of the course is stated, competences from Part C of the course are reviewed, and the outcome of the learning objectives is made clear; namely, that "the expected learning outcome is that the trainee ....." It should be noted that most of these same competences are found in Table A-VI/5 of the STCW Code along with methods for demonstrating competence and criteria for evaluating competence. Special attention should be given to the requirement therein for practical demonstrations of skill in conducting physical searches and non-intrusive inspections. Reference should also be made to 33 CFR Part 104 for a list of VSO competences.

Instructors should emphasize that no one is being trained to fight or similarly respond to security threats but rather that trainees should be able to identify, deter, or mitigate such actions through proper planning, preparation, and coordination with various entities.

1.3. Historical perspective

Trainees are most likely to appreciate the seriousness and proportions of the problem of security in general, and maritime security in particular, if they have a sense of the relevant history. Notable examples of security incidents should be relayed to this end. These might include the ACHILLE LAURO in 1985, Pan Am Flight 103 in 1988, the Mumbai bomb blasts of 1993, the World Trade Center bombing in 1993, the hijackings of the M.T. PETRO RANGER in 1998 and the M.V. ALONDRA RAINBOW in 1999, the bomb attack on the USS COLE in 2000, the hijacking of the M.V. INABUKWA in 2001, the terrorist attacks of September 11, 2001 on the World Trade Center and the Pentagon, the hijacking of the MT HAN WEI in 2002 and the explosion on board the LIMBURG in 2002.

1.4. Current security threats and patterns

Current threats to maritime security should be summarized in order to provide a basis for understanding of the recent conventions and legislation in this area and to fully grasp the importance of the training provided by this course. The prospective security officers receiving this training must clearly sense the reality of today's security issues, which include piracy, terrorism, contraband smuggling, cargo theft, and collateral damage. Some may have adopted a mindset that places the problem of security in the past or in such a remote corner that it appears distant or irrelevant. Before continuing on with the course this mindset should be identified and addressed.

Piracy and armed attacks continue to occur on a frequent basis. Attacks occur mostly in port areas, whereas piracy, by definition, usually occurs on ships at sea. The United Nations Convention on the Law of the Sea, Article 101, defines piracy as any of the following acts: illegal

acts of violence or detention or any act of depredation committed for private ends by the crew or the passengers of a private vessel or private aircraft and directed on the high seas against another vessel or aircraft or against persons or property on board such vessel or aircraft. It also includes such acts against a ship, aircraft, person or property in a place outside of the jurisdiction of any State.

Terrorism usually involves violence, or the threat of violence, by extremist groups seeking to gain political objectives by malicious means. A terrorist group may hope to make a statement by using various types of bombs, making bomb threats or hijacking a ship. Increasingly, terrorists are acting in connection with extremist religious sects that promote suicidal behavior.

Contraband smuggling, a criminal activity, may result in large financial loss to the ship owner whose vessel is being used by the smugglers. Often, drugs are the commodity being smuggled and they may be brought on board in a number of creative ways such as in luggage, stores, on or in a person's body, or in electronic equipment. Weapons are also a frequent item associated with smuggling. Like drugs, weapons, too, find their way on board in creative ways, such as in cargo containers.

Cargo theft, an age-old problem, continues to plague the maritime industry and causes financial losses in staggering amounts. Prevention is normally the most effective method of dealing with this security threat. The association between cargo theft and terrorism funding should be discussed. Instructors should convey that cargo theft is only one of the various threats to the security of cargo. Other such security threats should be discussed during this section of the course.

Collateral damage occurs when a nearby fire, explosion, or attack results in damage to a vessel or facility. While the damage is sometimes unintended, the costs are nevertheless real. Measures that may minimize the consequences of this type of damage should be discussed.

There are many elements of prevention, preparedness, response, and recovery that are common to transportation accidents, 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 in the Marine Transportation System, an "all-hazards" approach to maritime security training is recommended. Although not all emergencies are alike, where similar applications of technology, procedures, management strategies, etc., can be viewed as serving multiple purposes, the most rational and cost-effective use of security resources can be achieved. The integration of safety, security, and trade considerations in maritime security should be explained to trainees as an objective that will assist components of the Marine Transportation System to best defend against, and recover from, hazards of all kinds.

1.5. Vessel and port operations and conditions

This section of the course should provide trainees with sufficient understanding of the larger context in which maritime operations occur. Understanding the complex transportation and logistics framework of the maritime system will enable students to effectively undertake their security responsibilities. It is essential for students to have a basic understanding of the general patterns and mechanisms of cargo and passenger movement through international and intermodal transportation chains. The operational interfaces between maritime and other modes of transportation are a central component of this segment of the course. Trainees should also be exposed to the fundamentals of cargo tracking and related information systems in the context of security.

2. Maritime Security Policy

2.1. Relevant international conventions, codes, and recommendations

Trainees should appreciate the attempts by international bodies to minimize, stop, or otherwise control threats to security in maritime transportation. The International Maritime Organization (IMO) has adopted a number of resolutions and conventions to this end. For example, Resolution A.545(13)--Measures To Prevent Acts Of Piracy And Armed Robbery Against Ships was signed in 1983. In 1985 came IMO Resolution A.584 (14)--Measures To Prevent Unlawful Acts Which Threaten Safety Of Ships And Security Of Passengers (this was later reviewed in November of 2001 with IMO Resolution A.924(22)). Then in 1986 the IMO approved MSC/Circ.443--Measures To Prevent Unlawful Acts Against Passengers And Crew On Board Ships. In 1988, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) treaties aimed at ensuring that appropriate judicial action is taken against persons committing unlawful acts against ships. Unlawful acts include the seizure of vessels by force, acts of violence against persons on board vessels, and placing devices on board a vessel that are likely to destroy or damage it. The convention obliges contracting governments either to extradite or prosecute alleged offenders. The SUA came into effect on March 1, 1992.

Following the terrorist attacks in the United States on 11 September 2001, delegates at the twenty-second session of the IMO in November 2001 unanimously agreed to incorporate security regulations. They approved the development of new measures relating to the security of ships and facilities for adoption by a Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 in December 2002 (the Diplomatic Conference). This timetable of little more than a year represents a landmark achievement for IMO. It provides a clear indication of the gravity of the situation as well as the intention to protect world shipping against security incidents and threats.

The meeting of the Diplomatic Conference in December of 2002 resulted in amendments to SOLAS 74. These amendments enter into force on July 1, 2004. A brief summary of these amendments should be carried out with mention of changes to Chapter V but with emphasis on the changes to Chapter XI, Regulations 3 and 5 and the new Chapter XI-2 Regulations 1-13 and the ISPS Code. Since portions of the ISPS Code will be studied in more depth in later sections of the course, the summary here can be brief.

2.2. Relevant government legislation, regulations, and guidance

Trainees should be familiar 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 (SAFE) Port Act of 2006, the regulations contained in 33 CFR Chapter I, Subchapter H, and NVIC 03-07.

2.3. Definitions

Trainees will need a working knowledge of several terms found in SOLAS Chapter XI-2 Regulation 1, in the ISPS Code Part A section 2, and in 33 CFR Part 101. These terms may well need clarification from an experienced instructor in order for trainees to reach the necessary level of understanding.

2.4. Legal implications of action or non-action by security personnel

Action or non-action by security personnel is likely to have legal implications which may vary from one place to another and which are not entirely clear at this time. Personnel will have certain authorities and obligations yet they will also find that they face certain constraints. Instructors should carefully monitor developments locally and internationally along this line and be sure to bring the most recent information into each class as it is taught. Recent requirements brought about by the TWIC program most certainly present the potential for interesting legal issues and these should be discussed.

2.5. Handling sensitive security-related information and communications

Trainees should understand that certain information and communications will be considered security sensitive and that the level of sensitivity may change, as do MARSEC levels. Seemingly benign conversations, therefore, may result in disastrous consequences. All personnel will need to appreciate the risk of security leaks through communication by improper methods or to the wrong persons.

3. Security Responsibilities

This section is intended to give trainees a clear picture of the proportions of the maritime security system conceived of by the IMO, the U.S. Congress, the U.S. Coast Guard, and various federal agencies, and to show how the various entities will work together to form an efficient and effective whole.

3.1. Contracting governments

SOLAS Chapters XI-1 and XI-2 discuss the roles of the contracting governments and their obligations in the overall scheme to enhance maritime security. A brief understanding of this will help trainees to comprehend how and why the United States acted and how they may experience the Port State Control exercised by another government.

3.2. The company

The company is defined in 33 CFR Part 104 and SOLAS Chapter XI-1 and is given numerous obligations under SOLAS Chapter XI-2, the ISPS Code, and the domestic requirements, from Continuous Synopsis Records to the maintenance of the International Ship Security Certificate. The duties and responsibilities of the company are enumerated in 33 CFR Chapter I, Subchapter H. Trainees will benefit from a clear understanding of the role of the company and the support that they should expect from it.

3.3. The vessel

The term vessel as used here means a vessel to which 33 CFR Part 104 and Chapter XI of SOLAS apply. Various segments of Chapter XI, the ISPS Code, and 33 CFR Part 104 discuss the persons, activities, plans, documentation, and other elements that a vessel will be exposed to in the context of security. Trainees will need to understand these requirements as they relate to this important component of the Marine Transportation System.

3.4. The Master

Trainees should understand the important role of the Master in enhancing security and his/her duties and responsibilities in this regard. The instructor must convey the importance of the relationship between the SSO, the CSO, and the Master in the implementation of security measures. The authority of each position where security matters are concerned should be delineated.

3.5. The facility

The facility is defined in SOLAS Chapter XI-2 Regulation 1 part 1.9 and in 33 CFR Part 105. It is the location where the vessel-to-facility interface takes place. Given this, numerous duties and activities are assigned to the facility. Trainees should understand the roles and responsibilities of the facility in maintaining maritime security.

3.6- 3.11 Vessel Security Officer, Company Security Officer, Facility Security Officer, Vessel personnel with specific security duties, Facility personnel with specific security duties, and Other personnel

Trainees should understand the role of each of these persons and know what to expect from each in terms of authority and responsibility. The ISPS Code Parts A and B and relevant sections of 33 CFR Parts 104 and 105 clearly delineate the functions, duties, and training requirements for each of these categories of personnel. In the end these are the very people that will make security plans work and will recognize areas for improvement. They will each need to appreciate their own role as well as that played by others in the system.

4. Vessel Security Assessment

4.1. Risk assessment methodology

Vessel security assessment is an essential and integral part of the process of developing and updating the vessel security plan. In this segment of the course, it should be communicated to trainees that risk-based decision-making is central in the completion of security assessments and in the determination of appropriate security measures for a vessel. 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 to reduce the vulnerability 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.

Detailed guidance concerning methodologies for risk-based security assessment is provided in Part B of the ISPS Code and in U.S. Coast Guard documents.

4.2. Assessment tools

Trainees in the Vessel Security Officer course must be encouraged to adopt systematic and consistent approaches in the evaluation of security conditions and vulnerabilities. The focus of

the Vessel Security Officer in this regard will be more operational and less detailed than that of the Company Security Officer. The use of checklists to perform assessments of security in day-to-day operations should be discussed, noting the inclusion of categories such as the following:

- General layout of the vessel.
- Location of areas that should have restricted access, such as the bridge, engine room, radio room, etc., as well as those areas determined to be "secure" under the provisions of the TWIC program
- Location and function of each actual or potential access point to the vessel.
- Open deck arrangement including the height of the deck above water.
- Emergency and stand-by equipment available to maintain essential services.
- Numerical strength, reliability, and security duties of the vessel's crew.
- Existing security and safety equipment for protecting the passengers and crew.
- Existing agreements with private security companies for providing vessel and waterside security services.
- Existing protective measures and procedures in practice, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control and other appropriate systems.

4.3. On-scene security surveys

Trainees should be taught that the on-scene security survey is an integral part of any Vessel Security Assessment. They should understand that the survey should fulfil the following functions:

- identification of existing security measures, procedures and operations;
- identification and evaluation of key vessel operations that it is important to protect;
- identification of possible threats to key vessel operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and
- identification of weaknesses in the infrastructure, policies, and procedures.

It should be emphasized to course participants that the on-scene survey should examine and evaluate existing protective measures, procedures and operations for:

- ensuring the performance of all vessel security duties;
- monitoring restricted areas to ensure that only authorized persons have access;
- controlling access to the vessel, including any identification systems;
- monitoring of deck areas and areas surrounding the vessel;
- controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and the personal effects of vessel's personnel);
- supervising the handling of cargo and the delivery of vessel stores; and
- ensuring that vessel security communications capability, information, and equipment are readily available.

Such vessel surveys, assessments, and evaluations must be conducted in a manner that is mindful of the newer TWIC requirements as well as those stemming from the ISPS Code and domestic regulation.

4.4. Security assessment documentation

Trainees should understand that the Vessel Security Assessment shall be documented, reviewed, accepted, and retained by the company. Upon completion of the Vessel Security Assessment, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of vulnerabilities found during the assessment, and a description of counter measures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

5. Security Equipment

5.1. Security equipment and systems

Course participants should be aware of the types of security equipment and systems that are useful in enhancing maritime security, both ashore and afloat. Examples of such equipment include:

- AIS
- Ship Security Alert System
- Locks
- Lighting
- Handheld radios
- GMDSS equipment
- Closed Circuit Televisions
- Automatic Intrusion Detection Device (Burglar Alarm)
- Metal detectors
- Explosive detectors
- Baggage screening equipment
- Container X-ray devices
- General alarm
- TWIC readers

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 familiarity with the capabilities and appropriate deployment of such devices and systems. Trainees should be able to describe the use of information technology and communications systems in maintaining and enhancing security. The Company Security Officer and the Facility Security Officer may well be in a position to influence the purchase and installation of security equipment. Instructors are encouraged to discuss this possibility with trainees.

5.2. Operational limitations of security equipment and systems

The intent of this course segment is to communicate to trainees the functional limitations and operating constraints of security equipment that they may encounter or be called upon to use. 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. For the Vessel Security Officer, the focus should be on the tasks and procedures required to support such equipment while the vessel is at sea.

6. Vessel Security Plan

6.1. Purpose of the Vessel Security Plan

The Vessel Security Plan and requirements for its preparation and submission are defined in 33 CFR Part 104 and in the ISPS Code, Part A, Section 2.1. The VSP is a key element of efforts to maintain and enhance vessel and facility security. Therefore it is imperative that all candidates for the Vessel Security Officer and Company Security Officer positions fully understand the nature of the Vessel Security Plan. The Vessel Security Officer will need to maintain and supervise the implementation of the plan while the Company Security Officer will need to ensure that such a plan is developed, that it is submitted for approval, and thereafter that it is implemented and maintained. These are considerably different requirements and this course has addressed these differences in both content and time allotted for the subject. Trainees must understand the Coast Guard role in the approval of the Vessel Security Plan.

6.2. Contents of the Vessel Security Plan

The specific contents of the Vessel Security Plan are driven to a large degree by the results of the Vessel Security Assessment, and are therefore vessel-specific. Trainees should be familiar with the generic format of the VSP as defined by 33 CFR Part 104, thus knowing what to expect as they are assigned to various vessels and experience various Vessel Security Plans. It is suggested that a completed sample plan be provided by instructors to give trainees a better opportunity to understand the document to which they must be responsive aboard each vessel to which they are assigned as Vessel Security Officer.

6.3. Confidentiality issues

The Vessel Security Plan is to be considered sensitive security information and must be protected from unauthorized access or disclosure. Instructors should emphasize this and clearly delineate those few circumstances in which sections of the Vessel Security Plan may be inspected by Port State Control Officers.

6.4. Implementation of the Vessel Security Plan

Implementation of the Vessel Security Plan is a shared responsibility of the Company Security Officer and the Vessel Security Officer with the Vessel Security Officer being at the front line in this endeavor. Details concerning this shared responsibility should be presented in such as way as to not only ensure the understanding of the process but to also leave no doubt as to who is responsible for what. Both Vessel Security Officer and Company Security Officer must be clear on their roles in the implementation of the plan.

6.5. Maintenance and modification of the Vessel Security Plan

As written, the Vessel Security Plan is intended to address security measures for each of the three security levels but on further inspection it can be seen that the Vessel Security Plan is a living document and will require modification over time. Trainees must understand not only the provisions set out by the Vessel Security Plan but also their role in maintaining its effectiveness and contributing to positive modifications of the plan over time. Instructors should consider creating an exercise or a sample scenario showing the proper method of maintenance, identification of the need for modification, the proper route to follow for suggesting modifications, and the approval necessary before a modification or amendment can be set in place as new policy. As the TWIC program is set in motion, Vessel Security Plans will be modified to reflect the relevant requirements. Upon renewal of the VSP the U.S. Coast Guard will need to approve modifications that were made in order to comply with TWIC requirements.

7. Threat Identification, Recognition, and Response

7.1. Recognition and detection of dangerous substances and devices

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

7.2. Methods of screening, physical searches, and non-intrusive inspections

In this segment of the course, trainees will learn techniques used to conduct physical and non-intrusive screening and searches of persons, personal effects, vehicles, baggage, cargo, and vessel stores. Trainees should be informed that, unless there are clear security grounds for doing so; vessel and facility personnel should not be required to search their colleagues or their personal effects. It should be conveyed that any such search shall be undertaken in a manner that fully takes into account the human rights of the individual and preserves his or her basic human dignity. It is suggested that time be allotted so that each trainee can be given the opportunity to physically demonstrate his or her ability to conduct a search and a non-intrusive inspection. Not only is this lending value to the training, but it is also true that if the trainee is to be provided with a certificate of proficiency under Regulation VI/5 of the STCW Convention and Section A-VI/5 of the STCW Code, 1978, as amended, they must physically demonstrate these skills to meet the requirements for such certification.

7.3. Implementing and coordinating searches

Trainees should be taught that, to ensure that a thorough and efficient search is completed in the shortest possible time, search plans should be prepared in advance. 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.

Trainees should be acquainted with the utility of “check cards” in conducting systematic searches. For example, a “check card” is a card that can be issued to each searcher specifying the route to follow and the areas to be searched. These cards can be color-coded for different areas of responsibility, for example blue for deck, red for engine room. On completion of

individual search tasks, the cards are returned to a central control point. When all cards are returned, the search is known to be complete.

Course participants should be familiar with the list of basic equipment that may be employed in conducting searches. This list may include:

- flashlights and batteries;
- screwdrivers, wrenches and crowbars;
- mirrors and probes;
- gloves, hard hats, overalls and non-slip footwear;
- plastic bags and envelopes for collection of evidence;
- forms on which to record activities and discoveries.

Trainees should learn procedures to be followed so as to ensure effective and efficient searches. Examples of these include the following:

- Crew members and facility personnel should not be allowed to search their own areas in recognition of the possibility that they may have concealed packages or devices in their own work or personal areas
- The search should be conducted according to a specific plan or schedule and must be carefully controlled.
- Special consideration should be given to search parties working in pairs with one searching “high” and one searching “low”. If a suspicious object is found, one of the pair can remain on guard while the other reports the find.
- Searchers should be able to recognize suspicious items.
- There should be a system for marking or recording “clean” areas.
- Searchers should maintain contact with the search controllers, perhaps by UHF / VHF radio, bearing in mind the dangers of using non-intrinsically safe radio equipment in the vicinity of Improvised Explosive Devices (IEDs).
- Searchers should have clear guidance on what to do if a suspect package, device, or situation is found.
- Searchers should bear in mind that weapons and other dangerous devices may be intentionally placed to match their context as a means of disguise, such as a toolbox in an engine room.

Participants in the course should be acquainted with the fact that there are many places on board a vessel where weapons, dangerous substances, and devices can be concealed. Some of these are:

Cabins

- Back, sides, and underneath drawers
- Between bottom drawer and deck
- Beneath bunks, e.g. taped to bunk frame under mattress
- Under wash basin
- Behind removable medicine chest
- Inside radios, recorders, etc.

- Ventilator ducts
- Inside heater units
- Above or behind light fixtures
- Above ceiling and wall panels
- Cut-outs behind bulkheads, pictures, etc.
- False bottom clothes closets
- Among hanging clothes
- Inside wooden clothes hangers
- Inside rolled socks
- Hollowed-out molding

Companionways

- Ducts
- Wire harnesses
- Railings
- Fire extinguishers
- Fire hoses and compartments
- Access panels in deck, bulkheads, overhead

Toilet and Showers

- Behind and under washbasins
- Behind toilets
- In ventilation ducts and heaters
- Toilet tissue rollers, towel dispensers, supply lockers
- Taped to shower curtains, exposed piping, and light fixtures
- Access panels in deck, bulkheads, overhead

Deck

- Ledges on deck housing, electrical switch rooms, winch control panels
- Lifeboat storage compartments, under coiled rope, in deck storage lockers
- Paint cans, cargo holds, battery rooms, chain lockers.

Engine room

- Under deck plates
- Cofferdams, machinery pedestals, bilges
- Journal-bearing shrouds and sumps on propeller shaft
- Under catwalks, in bilges, in shaft alley
- Escape ladders and ascending area.

- In ventilation ducts, attached to piping, or in tanks with false gauges.
- Equipment boxes, emergency steering rooms, storage spaces.

Galleys and Stewards' Stores

- Flour bins and dry stores
- Vegetable sacks, canned foods (re-glued labels)
- Under or behind standard refrigerators
- Inside fish or sides of beef in freezers
- Bonded store lockers, slop chest, storage rooms.
- Behind or inside water coolers, ice chests, etc.

7.4. Recognition, on a non-discriminatory basis, of persons posing potential security risks

Instructors should explain suspicious patterns of behavior, while emphasizing the importance of avoiding racial profiling and ethnic stereotyping. Examples of suspicious behaviors include:

- Unknown persons photographing vessels or facilities.
- Unknown persons attempting to gain access to vessels or facilities.
- Persons attempting to gain access to secure areas with improper or suspect identification, including Transportation Worker Identity Cards.
- Individuals establishing businesses or roadside food stands either adjacent or in proximity to facilities.
- Unknown persons loitering in the vicinity of vessels or facilities for extended periods of time.
- Unknown persons telephoning facilities to ascertain security, personnel, or standard operating procedures.
- Vehicles with personnel in them loitering and perhaps taking photographs or creating diagrams of vessels or facilities.
- Small boats with personnel on board loitering and perhaps taking photographs or creating diagrams of vessels or facilities.
- General aviation aircraft operating in proximity to vessels or facilities.
- Persons who may be carrying bombs or participating in suicide squad activities.
- Unknown persons attempting to gain information about vessels or facilities by engaging personnel or their families in conversation.
- Vendors attempting to sell merchandise.
- Unknown workmen trying to gain access to facilities to repair, replace, service, or install equipment.
- E-mails attempting to obtain information regarding the vessel, facility, personnel, or standard operating procedures.
- Package drop-offs/attempted drop-offs.

- Anti-national sentiments being expressed by employees or vendors.
- Anti-national pamphlets or flyers distributed to employees or placed on windshields in parking lots.
- Out-of-the-ordinary phone calls.
- Recreational boaters or persons aboard refugee craft posing as mariners in distress to attract assistance from other vessels.

7.5. 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 the disabling of alarm systems, picking of locks, jamming of radio signals, use of false identification, etc.

7.6. Crowd management and control techniques

Course participants should be familiarized with the basic patterns of behavior of people in groups during time of crisis. The critical importance of clear communication with vessel personnel, facility personnel, passengers, and others involved should be underscored.

8. Vessel Security Actions

In general, the "vessel security actions" section of this course is material that both the Vessel Security Officer and the Company Security Officer should be very familiar with. The Facility Security Officer will need a slightly different level of understanding and the model course for Facility Security Officer varies in that respect. 33 CFR, Chapter I, Subchapter H and the ISPS Code are helpful in organizing material to be conveyed in this section of the course. Instructors should indicate that this section of the course is where ideas, plans, and preparation turn into actions and procedures.

8.1. Actions required by different security levels

The instructor should convey the different types of security measures that should be considered for vessels at sea and those in port as they respond to security threats and incidents and the various security levels that may be set. Requirements pertaining to vessel security incident procedures are delineated in 33 CFR Part 104. Trainees should be well-versed in the processes and procedures for crisis management and communications with emergency response providers and government agencies that are defined in the National Incident Management System (NIMS) and the National Response Framework (NRF). Trainees may benefit from an in-class creation of a checklist detailing the appropriate generic actions given various conditions.

8.2. Maintaining security of the vessel-to-port and vessel-to-facility interfaces

The vessel-to-port and vessel-to-facility interfaces are defined in 33 CFR Part 101 and SOLAS Chapter XI-2 Regulation 1. It is the vessel-to-facility interface that determines that a facility exists and therefore determines the need for a Facility Security Plan and the interaction with the Vessel Security Plan. The setting of security levels by the port or by the vessel, with liaison

services provided by the Company Security Officer, will allow the Facility Security Officer and the Vessel Security Officer to understand their duties and constraints. Instructors should ensure that trainees are clear on the critical importance of the interaction between the Vessel Security Plan and the Facility Security Plan. A paramount objective of this section of the course is ensuring that trainees understand the need to be familiar with, and adhere to, established procedures for interfacing with ports, facilities, and other vessels at all MARSEC levels.

8.3. Usage of the Declaration of Security

The Declaration of Security is defined in 33 CFR Subchapter H and in Regulation 1 of SOLAS Chapter XI-1. 33 CFR Part 104 and the ISPS Code further describe the function of the Declaration of Security, when it should be completed, who may initiate it, and who is required to sign it. There is a sample Declaration of Security in Appendix 1 of Part B of the ISPS Code, which may be helpful in explaining the nature and use of the Declaration of Security. It should be conveyed that manned vessels must maintain copies of the last 10 Declarations of Security and a copy of each continuing DoS for at least 90 days after the end of its effective period. The DoS is among the security-related records that must be kept by the VSO for at least two years and that must be made available to the Coast Guard upon request.

8.4. Implementation of security procedures

Building on the understanding gained from previous sections in this course, trainees should be ready to synthesize the requirements and plans into actual procedures such as security inspections, controlling access to the vessel, monitoring deck areas and areas surrounding the vessel, and so forth.

8.5. Access control

Normal access control measures may be enhanced by the TWIC program requirements on escorting, secure areas, and checks for personal identification, including inspection of credentials. These requirements are critical to understand and meet for complete and effective access control. Reference should be made to 33 CFR Part 104 as well as to NVIC 03-07

9. Emergency Preparedness, Drills, and Exercises

9.1. Contingency planning

This portion of the course is concerned with incident response planning for a variety of contingencies associated with terrorism, other criminal activities, and other emergencies that may arise in the maritime setting. Appropriate action to be taken in the case of bomb threats, explosions, piracy, hijackings, and similar events should be discussed.

9.2. Security drills and exercises

It should be conveyed to course participants that the objective of drills and exercises is to ensure that vessel personnel are proficient in all assigned security duties at all security levels and in the identification of any security related deficiencies that need to be addressed.

Trainees should learn that the effective implementation of the provisions of the vessel security plan requires that drills be conducted at least once every three months. In addition, in cases where more than 25 percent of the vessel's personnel have been changed, at any one time,

with personnel who have not previously participated in any drill on that vessel within the last three months, a drill should be conducted within one week of the change. These drills should test individual elements of the plan such as:

- damage to, or destruction of, the vessel or facility, e.g. by explosive devices, arson, sabotage or vandalism;
- hijacking or seizure of the vessel or of persons on board;
- tampering with cargo, essential vessel equipment or systems, or ship's stores;
- unauthorized access or use, including presence of stowaways;
- smuggling weapons or equipment, including weapons of mass destruction;
- use of the vessel to carry persons intending to cause a security incident, or their equipment;
- use of the vessel itself as a weapon or as a means to cause damage or destruction;
- attacks from seaward while at berth or at anchor; and
- attacks while at sea.

Various types of exercises that may include participation of Vessel Security Officers, Company Security Officers, Facility Security Officers, government authorities, and other relevant personnel should be carried out at least once each calendar year with no more than 18 months between exercises. These exercises should test communications, coordination, resource availability, and response. These exercises may be:

- full scale or live;
- tabletop simulation or seminar; or
- combined with other exercises held such as search and rescue or emergency response exercises.

9.3. Assessment of security drills and exercises

At the end of each drill or exercise, the Vessel Security Officer shall review the drill or exercise, and ensure that any mistakes made or deficiencies identified are corrected. All personnel involved shall give their comments on the effectiveness of the drill to the Vessel Security Officer.

10. Security Administration

10.1. Documentation and records

Drawing on 33 CFR Part 104 and Chapter XI-1 Regulation 5 and Chapter XI-2 of SOLAS and Section 10 of the ISPS Code, the instructor will find sufficient references to, and examples of, required documents as well as requirements for record keeping. Records of activities addressed in the Vessel Security Plan must be kept on board for certain time periods that are determined by administrations. Pertinent records include, but are not limited to, the following:

- International Ship Security Certificate,
- the Continuous Synopsis Record and related documents;
- Declaration of Security;
- records of drills;

- records of incidents and breaches of security;
- records of training sessions; and
- formal training records.

10.2. Reporting security incidents

Trainees will appreciate that all security incidents, including TWIC violations, must be reported in accordance with specific reporting requirements and the applicable security plan. Obligations of owners and operators pertaining to reporting are identified in 33 CFR Part 101. It may be helpful to for instructors to provide several sample security incidents and have the class or individuals explain how they would go about reporting these incidents.

10.3. Monitoring and control

Here the focus of monitoring is on the Vessel Security Plan itself. Proper administration of the plan indicates that the Master, the Vessel Security Officer, and the Company Security Officer should review the Vessel Security Plan and measure its overall effectiveness and relevance over time.

10.4. Security audits and inspections

33 CFR Chapter I, Subchapter H provides detail regarding control and compliance measures that may be employed by the U.S. Coast Guard Captain of the Port, as are the various requirements associated with audits of the VSP for which the VSO and/or CSO are responsible.

10.5. Reporting nonconformities

The audit, inspection, and periodic review process required by the ISPS Code and 33 CFR Chapter I, Subchapter H naturally calls for a means of identifying, communicating, and rectifying non-conformities. Both the Vessel Security Officer and the Company Security Officer play key roles in this effort to keep the Vessel Security Plan in an optimum condition.

11. Security Training

11.1. Training requirements

The training requirements set out under the ISPS Code can be found in Parts A and B of the Code and in 33 CFR Chapter I, Subchapter H, and should be explained briefly to trainees. Instructors should clarify the requirements defining who needs to be trained, what the training consists of, and where the responsibility lies for the training of various persons involved in maritime security.

Part E: Evaluation

Introduction

The effectiveness of any evaluation depends on the accuracy of the description of what is to be measured.

The learning objectives that are used in the detailed teaching syllabus will provide a sound base for the construction of suitable tests for evaluating trainee progress.

Method of evaluation

The methods chosen to carry out an evaluation will depend upon what the trainee is expected to achieve in terms of knowing, comprehending and applying the course content.

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

Where the course content is aimed at the acquisition of practical skills, the test would involve a practical demonstration by the trainee making use of appropriate equipment, tools, etc.
The responses demanded may therefore consist of:

- 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.
- carrying out calculations to solve numerical problems
- the writing of an essay or report.

Validity

The evaluation must be based on clearly defined objectives, and it must truly represent what is to be measured. There must be a reasonable balance between the subject topics involved and also in the testing of trainees' KNOWLEDGE, COMPREHENSION, and APPLICATION of concepts.

The time allocated for the trainee to provide a response is very important. Each question or task must be properly tested and validated before it is used to ensure that the test will provide a fair and valid evaluation.

Reliability

To be reliable, an evaluation procedure should produce reasonably consistent results no matter which set of papers or version of the test is used.

■ Subjective testing

Traditional methods of evaluation require the trainee to demonstrate what has been learned by stating or writing formal answers to questions.

Such evaluation is subjective in that it invariably depends upon the judgment of the evaluator. Different evaluators can produce quite different scores when marking the same paper or evaluating oral answers.

■ Objective testing

A variety of objective tests have been developed over the years. Their common feature is that the evaluation does not require a judgment by the evaluator. 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 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, or they may be of the true/false type or of the multiple-choice type.

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 must select the most appropriate.

■ 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).

■ Guess factor

The ‘guess factor’ with four alternative responses in a multiple-choice test would be 25%. The passing score chosen for all selective-response questions should take this into account.

■ Scoring

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

A more sophisticated scoring technique entails awarding one point for a correct response, zero for a nil 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.

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