U.S. Department of Transportation
Maritime Administration

Maritime Security for Facility Personnel with Specific Security Duties

Model Course MTSA 04-02

Prepared by

THE UNITED STATES MERCHANT MARINE ACADEMY

December 2004

Contents

Foreword

This course is one of a series developed by the U.S. Maritime Administration in fulfilment 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 me 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 of 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. The Ship Security Officer, Company Security Officer, and Port Facility Security Officer courses have been published by the IMO and are now the global benchmark for maritime security training in their respective areas.

In a style similar to the IMO model courses, the course that follows is one of four based on the MARAD Report to Congress that provide training guidance for security personnel not addressed by the IMO model courses. In addition to informing and helping to standardize maritime security training, this course is one that will be used as a reference in the interim system of course approval and certification that has been jointly established by MARAD and the U.S. Coast Guard. Organizations that wish to submit maritime security courses for approval under this system should use this course, the others in the MTSA series, and the three IMO model courses as the standard reference for the development and operation of courses in this domain.

It is my hope that this course and the others like it will serve to harmonize and standardize port, maritime, and intermodal transportation security education and training, and that this will enhance the security of our Nation.

Captain William G. Schubert
Maritime Administrator

Introduction

This model course is intended as specific guidance upon which education and training providers can immediately 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 other pertinent guidance are addressed through standards of knowledge 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. Input thus received has helped to ensure that the model course is fully consistent with applicable law enforcement, government, and industry standards.

This model course and others in the series of which it is a part constitute a base-level curriculum for maritime security education and training that includes those subjects listed in MTSA Sec. 109 (b)(2). In addition to delineating the duties and responsibilities of personnel in various categories and identifying the subject areas that should be contained in education and training that are intended to be responsive to these 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 Sec. 109 (b)(2).

This course is also intended to serve as a comparison reference for courses that are submitted for approval under the MARAD/USCG MTSA Section 109 course approval system. It should be noted in this connection that U.S. domestic training courses for Vessel Security Officer, Company Security Officer, and Facility Security Officer should use the IMO model courses for Ship Security Officer (Model Course 3.19), Company Security Officer (Model Course 3.20), and Port Facility Security Officer (Model Course 3.21), respectively, as standards for course content, schedule, and related matters.

Part A: Course Framework

Scope

This model course is intended to provide the knowledge required for facility personnel who are assigned specific security duties in connection with a Facility Security Plan (FSP) to perform their duties in accordance with the requirements the Maritime Transportation Security Act of 2002 and/or Chapter XI-2 of SOLAS 74 as amended and/or the IMO ISPS Code and/or U.S. Coast Guard regulations contained in 33 CFR Chapter 1 Subchapter H.

Objective

Those who successfully complete the course should be able to demonstrate sufficient knowledge to undertake the duties assigned under the FSP. This knowledge shall include, but is not limited to:

1. knowledge of current security threats and patterns;
2. recognition and detection of weapons, dangerous substances and devices;
3. recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security;
4. techniques used to circumvent security measures;
5. crowd management and control techniques;
6. security related communications;
7. knowledge of emergency procedures and contingency plans;
8. operation of security equipment and systems;
9. testing, calibration and maintenance of security equipment and systems;
10. inspection, control, and monitoring techniques; and
11. methods of physical searches of persons, personal effects, baggage, cargo, and vessel stores.

Entry standards

It is assumed that those attending this course will be persons employed (or to be employed) by a port facility operator and are likely to be assigned specific security duties in connection with the Facility Security Plan. Training providers must verify trainee identity and citizenship.

Course certificate, diploma or document

Following verification of identity and citizenship, documentary evidence should be issued to those who have successfully completed this course indicating that the holder has completed training in "Maritime Security for Facility Personnel with Specific Security Duties" based on this model course.

Course delivery

The outcome 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 should depend on the facilities and equipment available, bearing in mind the aims and objectives of this course.

Staff requirements

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 shipboard environments (vessels or mock-ups) for certain segments of the course may enhance the overall effectiveness of this training.

.

Teaching aids

Course Framework (Part A of the course)

Instructor Manual (Part D of the course)

Audiovisual aids: video cassette player, TV, slide projector, overhead projector, etc.

Photographs, models, or other representations of various vessels and vessel parts to illustrate operational elements and security vulnerabilities.

Video cassette(s)

Distance learning package(s)

Bibliography

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

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

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

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

United States Department of Transportation. (1997). *Port Security: A National Planning Guide.* Washington, D.C.: U.S. DOT.

United States Department of Transportation. (1998). *Port Security: Security Force Management.* Washington, D.C.: U.S. DOT.

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.

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

Instruments, legislation, and regulatory references

International Labour Organization. *Seafarers' Hours of Work and the Manning of Ships Convention, 1996.* (No. 180).

International Labour Organization. *Seafarers' Identity Documents Convention, 195*8. (No. 108).

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

International Maritime Organization. (2001). *International Convention for the Safety of Life at Sea (SOLAS), 1974*. London: IMO. (IMO-IC110E).

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

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

Commandant, United States Coast Guard. (2002, September). "Guidelines for Port Security Committees and Port Security Plans Required for U.S. Ports." Navigation and Vessel Inspection Circular No. 9-02.

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

Commandant, United States Coast Guard. (2003, 13 January). "Recommended Security Guidelines for Facilities." Navigation and Vessel Inspection Circular No. 11-02.

Coast Guard, Department of Homeland Security. (2003, 22 October). *33 CFR (Navigation and Navigable Waters), Chapter 1, Subchapter H—Maritime Security, Parts 101, 103, 104, 105, 106.*

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

■ Textbooks

None recommended at this time.

Part B: Course Outline

	Subject Area	Hours
	Introduction	1.0
	1.1 Course overview	
	1.2 Competences to be achieved	
	1.3 Current security threats and patterns	
	1.4 Vessel and port operations and conditions	
2	**Maritime Security Policy**	0.75
	2.1 Relevant international conventions, codes, and recommendations	
	2.2 Relevant government legislation and regulations	
	2.3 Definitions	
	2.4 Handling sensitive security-related information and communications	
3	**Security Responsibilities**	1.25
	3.1 Contracting governments	
	3.2 Recognized Security Organizations	
	3.3 The company	
	3.4 The vessel	
	3.5 The port 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	**Facility Security Assessment**	1.0
	4.1 Assessment tools	
	4.2 On-scene security surveys	
	4.3 Security assessment documentation	

5	**Security Equipment**	0.75
	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	**Threat Identification, Recognition, and Response**	1.25
	6.1 Recognition and detection of weapons, dangerous substances and devices	
	6.2 Methods of physical searches and non-intrusive inspections	
	6.3 Execution and coordination of searches	
	6.4 Recognition, on a non-discriminatory basis, of persons posing potential security risks	
	6.5 Techniques used to circumvent security measures	
	6.6 Crowd management and control techniques	
7	**Facility Security Actions**	0.75
	7.1 Actions required by different security levels	
	7.2 Maintaining security of the vessel/port interface	
	7.3 Familiarity with the Declaration of Security	
	7.4 Execution of security procedures	
8	**Emergency Preparedness, Drills, and Exercises**	0.75
	8.1 Execution of contingency plans	
	8.2 Security drills and exercises	
9	**Security Administration**	0.5
	9.1 Documentation and records	
	Total:	8.0

Facility Personnel with Specific Security Duties
Course Timetable

Day/Period	1st Period (2.0 hours)	2nd Period (2.0 hours)	3rd Period (2.0 hours)	4th Period (2.0 hours)
Day 1	**1 Introduction** 1.1 Course overview 1.2 Competences to be achieved 1.3 Current security threats and patterns 1.4 Vessel and port operations and conditions **2 Maritime Security Policy** 2.1 Relevant international conventions, codes, and recommendations 2.2 Relevant government legislation and regulations 2.3 Definitions 2.4 Handling sensitive security-related information and communications **3 Security Responsibilities** 3.1 Contracting governments 3.2 Recognized Security Organizations	3.3 The company 3.4 The vessel 3.5 The port 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 Facility Security Assessment** 4.1 Assessment tools 4.2 On-scene security surveys 4.3 Security assessment documentation	**5 Security Equipment** 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 Threat Identification, Recognition, and Response** 6.1 Recognition and detection of weapons, dangerous substances and devices 6.2 Methods of physical searches and non-intrusive inspections 6.3 Execution and coordination of searches 6.4 Recognition, on a non-discriminatory basis, of persons posing potential security risks 6.5 Techniques used to circumvent security measures 6.6 Crowd management and control techniques	**7 Facility Security Actions** 7.1 Actions required by different security levels 7.2 Maintaining security of the vessel/port interface 7.3 Familiarity with the Declaration of Security 7.4 Execution of security procedures **8 Emergency Preparedness, Drills, and Exercises** 8.1 Execution of contingency plans 8.2 Security drills and exercises **9 Security Administration** 9.1 Documentation and records

Part C: Detailed Teaching Syllabus

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 ....."

Learning Objectives

1. Introduction (1.0 hour)

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. Current security threats and patterns

.1 summarizes threats to the maritime transportation industry, such as:

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

1.4. 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 (0.75 hour)

2.1. Familiarity with relevant international conventions, codes, and recommendations

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

.2 summarizes the rapidity with which IMO acted to enhance maritime security following 9/11

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

2.2. Familiarity with relevant government legislation and regulations

.1 summarizes the requirements of relevant national legislation and regulations.

2.3. Definitions

.1 defines

- Vessel Security Plan
- Company Security Officer

- Vessel Security Officer
- Port facility
- Vessel-to-facility interface
- Vessel-to-port interface
- Vessel-to-vessel activity
- Facility Security Officer
- Designated Authority
- Recognized Security Organization
- Declaration of Security
- Security incident
- Security Level
- the three security levels

2.4. Handling sensitive security-related information and communications

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

3. **Security Responsibilities** (1.25 hours)

3.1. Contracting governments

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

3.2. Recognized Security Organizations

.1 surveys the role of the Recognized Security Organization

3.3. The company

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

- ensuring 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

3.4. The vessel

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

3.5. The facility

.1 states that facilities shall comply with the relevant requirements of the Maritime Transportation Security Act of 2002 and/or Chapter XI-2 of SOLAS 74 as amended and/or the IMO ISPS Code and/or U.S. Coast Guard regulations contained in 33 CFR Chapter 1 Subchapter H

.2 states that the facility shall act upon the security levels set by the Administration

3.6. Vessel Security Officer

.1 states that the company shall designate a Vessel Security Officer for each vessel

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

3.7. Company Security Officer

.1 states that the company shall designate a Company Security Officer

.2 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 is responsible

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

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

3.8. Facility Security Officer

.1 states that the 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 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 other than the VSO 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. Facility Security Assessment (1.0 hour)

4.1. Assessment tools

.1 discusses the use of checklists in conducting security assessments

4.2. 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 facility layout

.4 divides the survey into the following sections:

- Physical Security
- Structural Integrity
- Personnel Protection Systems
- Procedural Policies
- Radio and Telecommunication Systems
- Relevant Transportation Infrastructure
- Utilities
- Other Areas

.5 discusses the importance and elements of physical security in port facilities

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

.7 discusses the components and operations of systems to protect facility personnel

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

.9 describes the use of information technology and communications systems in port facility operations and in maintaining security

.10 identifies other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations within the port facility

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

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

5. **Security Equipment** (0.75 hour)

5.1. Security equipment and systems

.1 demonstrates familiarity with 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. Threat Identification, Recognition, and Response (1.25 hours)

6.1. Recognition and detection of weapons, dangerous substances and devices

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

6.2. Methods of physical searches and non-intrusive inspections

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

6.3. Execution and coordination of searches

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

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

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

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

.5 summarizes the various places of concealment in a port facility

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

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

.2 states how important it is to be observant to recognize such persons

6.5. Techniques used to circumvent security measures

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

6.6. Crowd management and control techniques

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

.2 summarizes the importance of clear communication with facility personnel and others during an emergency

7. Facility Security Actions (1.0 hour)

7.1. Actions required by different security levels

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

7.2. Maintaining security of the vessel/port interface

.1 lists the reporting requirements for vessels prior to entering port

7.3. Familiarity with the Declaration of Security

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

7.4. Execution of security procedures

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

- ensure the performance of all facility security duties
- control access to the facility
- control the embarkation of persons and their effects
- monitor restricted areas to ensure only authorized persons have access
- coordinate the security aspects of the handling of cargo and vessel stores; and
- ensure that security communication is readily available

8. Emergency Preparedness, Drills, and Exercises (0.75 hour)

8.1. Execution of contingency plans

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

.2 discusses contingency plans for:

- hijacking
- bomb threat
- unidentified objects / explosives on vessel
- damage to / destruction of facility
- piracy and other depredations
- stowaways

8.2. Security drills and exercises

.1 states the requirements for conducting drills and exercises

9. Security Administration (0.5 hour)

9.1. Documentation and records

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

.2 states the activities for which records shall be kept and the duration for which they should be retained.

Total: 8.0 hours

Part D: Instructor Manual

The instructor manual provides guidance on the material that is to be presented during the course for Facility Personnel with Specific Security Duties. 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 nine main headings:

1 Introduction

2 Maritime Security Policy

3 Security Responsibilities

4 Facility Security Assessment

5 Security Equipment

6 Threat Identification, Recognition, and Response

7 Facility Security Actions

8 Emergency Preparedness, Drills, and Exercises

9 Security Administration

The course outline and timetable provide guidance on the time allocation for the course material, but the instructor is free to modify this if it is deemed necessary. The detailed teaching syllabus must be studied carefully and, where appropriate, lesson plans or lecture notes compiled.

Preparation and planning are the most important criteria in effectively presenting this course. Availability and proper use of course materials are 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 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 should be a brief statement of the purpose of the course, a short review of the timeline, an introduction of 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 ....."

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 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. Prospective security personnel 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 an all too frequent basis. Attacks occur mostly in port areas, whereas piracy, by definition, usually involves ships at sea. In fact, 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 vessel, 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 vessel. 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 vessel 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 various 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.

Although there may not be violence or political issues involved in most cargo theft cases, this matter remains high on the list of security threats and requires solutions discussed in this course. 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. There are measures that may minimize the consequences of this type of damage.

1.4 Vessel and port operations and conditions

This section of the course should provide trainees with an understanding of the larger context in which maritime operations occur. Familiarity with 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 interface between maritime and other modes of transportation is 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 would include the seizure of vessels by force, acts of violence against persons on board vessels, and placing devices on board a vessel which 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 tragic events of September 11, 2001 the twenty-second session of the IMO, in November of 2001, unanimously agreed to incorporate security regulations. They approved the development of new measures relating to the security of vessels and of port facilities for adoption by a Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 in December of 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 and regulations

The Maritime Transportation Security Act of 2002, the maritime security regulations contained in 33 CFR Chapter 1 Subchapter H, and other pertinent legislation and guidance should be summarized for trainees.

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 Chapter 1 Subchapter H. These terms may well need clarification from an experienced instructor in order for trainees to reach the necessary level of understanding. For instance, it might require emphasis or other clarification by the instructor to establish that the Vessel Security Officer is a person on board the vessel and in that sense it may be impossible for a Company Security Officer to also act as the Vessel Security Officer.

2.4 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 levels of security 1, 2, and 3. 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 as implemented via the MTSA regulations and to show how the various entities will work together to form an efficient and effective whole.

3.1 Contracting governments

Instructors should discuss the roles of contracting governments and their obligations in the international scheme to enhance maritime security. A brief understanding of this subject will help trainees to comprehend how and why the United States has acted and how they may experience port state control as exercised by another government.

3.2 Recognized Security Organizations

The trainee should understand that an RSO may take on the security-related activities of a contracting government.

3.3 The company

The company is defined in 33 CFR Subchapter H and by SOLAS Chapter XI-1. Companies are given numerous obligations under SOLAS Chapter XI-2 and the ISPS Code and/or 33 CFR Subchapter H, ranging from requirements for Continuous Synopsis Records to the maintenance of the International Ship Security Certificate. Trainees will benefit greatly from a clear understanding of the role of the company and the support that they should expect from the company.

3.4 The vessel

The term vessel as used here means any and all vessels to which the provisions of 33 CFR Chapter 1 Subchapter H apply. Segments of Chapter XI and the ISPS Code pertain to some of these vessels and discuss the persons, activities, plans, documentation and so forth that vessels subject to SOLAS will be exposed to in a security context. All trainees will nevertheless need to understand the requirements relating to the security of the vessel in its role as the cornerstone of the marine transportation system.

3.5 The facility

The facility is defined in Chapter XI-2 of SOLAS 74 as amended, the ISPS Code, and/or the U.S. Coast Guard regulations contained in 33 CFR Chapter 1 Subchapter H. It is the location where the vessel/facility interface takes place. As such, numerous duties and responsibilities are assigned to the facility. All trainees should understand the role of the facility in maintaining the security of the maritime transportation system.

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 various persons and know what to expect from each in terms of authority and responsibility. 33 CFR Chapter 1 Subchapter H and/or Parts A and B of the ISPS Code 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 who are best positioned to recognize areas for improvement. They will each need to appreciate their own role as well as that played by the others.

4 Facility Security Assessment

4.1 Assessment tools

Trainees must be encouraged to adopt systematic and consistent approaches to the evaluation of security conditions and vulnerabilities. Facility personnel with specific security duties may be called upon to assist in these evaluations. The use of checklists to perform assessments of security in day-to-day operations should therefore be discussed, noting the inclusion of categories such as the following:

- physical security;
- structural integrity;
- personnel protection systems;
- procedural policies;
- radio and telecommunication systems, including computer systems and networks;
- relevant transportation infrastructure;
- utilities; and
- other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations within the port facility

4.2 On-scene security surveys

Trainees should be taught that the on-scene security survey is an integral part of any Facility Security Assessment. They should understand that the survey examines and evaluates existing facility protective measures, procedures, and operations to verify and collect information pertaining to the following:

- The general layout of the facility;
- The location and function of each actual or potential access point to the facility;
- Existing protective measures including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems;
- 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;
- 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.

5 Security Equipment

5.1 Security equipment and systems

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

- AIS
- Vessel 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

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 of such devices and systems. Instructors should stress the need for familiarization training involving the specific security equipment in each facility.

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.

6 Threat Identification, Recognition, and Response

6.1 Recognition and detection of weapons, dangerous substances and devices

The focus of this segment of the course 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.

6.2 Methods of physical searches and non-intrusive inspections

In this segment of the course, trainees will learn techniques used to conduct physical and non-intrusive searches of persons, personal effects, 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.

6.3 Execution and coordination of searches

Trainees should be acquainted with the utility of "check cards" in conducting systematic searches. 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 colour-coded for different areas of responsibility within the port facility. 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. The findings of the search can then be discussed.

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:

- 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 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 its 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 in port facilities where weapons, dangerous substances, and devices can be concealed. Some of these are:

- Behind removable medicine chest

- Inside radios, recorders, etc.
- In cargo containers
- Ventilator ducts
- Storage tanks
- Inside heater units
- Above or behind light fixtures
- Above ceiling and wall panels
- False bottom clothes closets-hanging clothes
- Inside wooden clothes hangers
- Inside rolled socks, spare socks
- Hollowed-out molding
- Ducts
- Wire harnesses
- Railings
- Fire extinguishers
- Fire hoses and compartments
- Access panels in floors, walls, ceilings
- Behind or inside water coolers, igloos
- 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 floors, walls, ceiling

6.4 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 behaviours include:

- Unknown persons photographing vessels or facilities.
- Unknown persons attempting to gain access to vessels or facilities.
- Individuals establishing businesses or roadside food stands either adjacent or in proximity to facilities.
- Unknown persons loitering in the vicinity of vessels or port 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 walking up to personnel or their families and engaging them in a conversation.
- Vendors attempting to sell merchandise.
- Workmen trying to gain access to facilities to repair, replace, service, or install equipment.
- E-mails attempting to obtain information regarding the 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.

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 the disabling of alarm systems, picking of locks, jamming of radio signals, etc.

6.6 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.

7 Facility Security Actions

33 CFR Chapter 1 Subchapter H and Parts A and B of the ISPS Code will be 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.

7.1 Actions required by different security levels

The instructor should convey the different types of security measures that should be considered for facilities and vessels as they respond to security incidents and the various security levels that may be set. Trainees may benefit from the in-class creation of checklists detailing the appropriate generic actions given various conditions. The importance of familiarization training involving the Facility Security Plan particular to each facility should be emphasized.

7.2 Maintaining security of the vessel/port interface

The vessel/port interface determines the need for a Facility Security Plan and the interaction with the Vessel Security Plan. Instructors should ensure that trainees are clear on the critical importance of the interaction between the vessel security plan and that of the facility.

7.3 Familiarity with the Declaration of Security

The Declaration of Security is defined in Regulation 1 of SOLAS Chapter XI-1 and in 33 CFR Chapter 1 Subchapter H. 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.

7.4 Execution 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 facility, ensuring the screening of unaccompanied baggage, and so forth.

8 Emergency Preparedness, Drills, and Exercises

8.1 Execution of contingency plans

This portion of the course is concerned with the implementation of plans for a variety of contingencies associated with terrorism and other criminal activities that may arise in the maritime setting. Possible responses in the case of bomb threats, explosions, piracy, hijackings, and similar events should be discussed.

8.2 Security drills and exercises

It should be conveyed to course participants that the objective of drills and exercises is to ensure that facility 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 effective implementation of the provisions of the Facility Security Plan requires that drills be conducted at least once every three months. These drills should test individual elements of the plan such as:

- damage to, or destruction of, a vessel or port facility, e.g. by explosive devices, arson, sabotage or vandalism;
- hijacking or seizure of a vessel or of persons on board;
- tampering with cargo, essential facility equipment, systems, or vessel stores;
- unauthorized access to or use of facility structures or equipment;

- smuggling weapons or equipment, including weapons of mass destruction;
- use of a vessel to carry persons intending to cause a security incident, or their equipment;
- use of vessels as weapons or as a means to cause damage or destruction; and
- nuclear, biological and chemical attack.

Various types of exercises involving participation of facility security personnel should be carried out at least once each calendar year with no more than 18 months between the 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 Security Administration

9.1 Documentation and records

Drawing on 33 CFR Chapter 1 Subchapter H and SOLAS Chapter XI-1 Regulation 5 and Chapter XI-2, the instructor will find references to, and examples of, required documents as well as requirements for record keeping. Record-keeping requirements associated with the Facility Security Plan should be summarized.

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, by viva-voce or objective tests
- 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 judgement 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 judgement 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 pass mark chosen for all selective-response questions should take this into account.

■ Scoring

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

A more sophisticated scoring technique entails awarding one mark 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 mark and a 75% chance of losing one mark.

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