U.S. Department of Transportation
Maritime Administration

Maritime Security for Military, First Responder, and Law Enforcement Personnel

---

Model Course MTSA 05-01

Prepared by

THE UNITED STATES MERCHANT MARINE ACADEMY

18 October 2005

Contents

FOREWORD I
INTRODUCTION 1
PART A: COURSE FRAMEWORK 1
PART B: COURSE OUTLINE 6
PART C: DETAILED TEACHING SYLLABUS 11
PART D: INSTRUCTOR MANUAL 19
PART E: EVALUATION 32

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 stemming from 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.

The Maritime Administration gratefully acknowledges the contributions to the development of this course made by the Department of Homeland Security's Federal Law Enforcement Training Center (FLETC). FLETC and the U.S. Merchant Marine Academy jointly conducted a training needs assessment survey and held an important national conference to solicit the input of military first responder, and law enforcement personnel on draft training curricula and training requirements.

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.

John Jamian
Acting 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 military, first responder, and law enforcement personnel without prior maritime background to conduct their duties aboard vessels, in port facilities and elsewhere in the marine environment in accordance with the requirements of the Maritime Transportation Security Act of 2002.

Objective

The principal objective of this course is to provide military, first responder, and law enforcement personnel with an understanding of enhancements to security in the maritime arena and the unique circumstances and operational conditions that prevail therein.
Those who successfully complete the course should better be able to undertake their duties and responsibilities as military, first responder and law enforcement personnel in the port, maritime, and intermodal context, which may include, but are not limited to:

1. inspecting vessels, terminals, and other facilities;
2. responding to crises involving threats of terrorism or actual attacks;
3. monitoring and controlling access to facilities and vessels;
4. interviewing, examining, and credentialing transportation workers and facility personnel;
5. conducting surveillance operations and participating in undercover assignments;
6. tracking and interdicting suspicious cargo, persons, vessels, or vehicles;
7. recognizing and detecting the presence of bombs, explosives, and Weapons of Mass Destruction;
8. interacting on security matters with Vessel Security Officers, Company Security Officers, Facility Security Officers, and relevant federal, state, and local agencies; and
9. performing threat, risk, and vulnerability assessments; security planning; and contingency planning.

Entry standards

It is assumed that those attending this course will be experienced military, first responder, or law enforcement personnel. 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 Military, First Responder, and Law Enforcement Personnel" 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, 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 actual or simulated vessel and facility environments 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.

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

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, 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 (T)

None recommended at this time.

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	
2	**Maritime, Intermodal, and Supply Chain Conditions and Operations**	3.5
2.1	Maritime orientation and definitions	
2.2	Supply chain and intermodal transportation system structure and operations	
2.3	Port and transportation information and tracking systems	
2.4	Cargo and transportation documentation	
2.5	Hazardous materials security	
2.6	Port and maritime security measures	
3	**Maritime Security Policy**	1.0
3.1	Relevant international conventions, codes, and recommendations	
3.2	Relevant government legislation and regulations	
3.3	Definitions	
3.4	Legal implications of action or non-action by security personnel	
3.5	Handling sensitive security-related information and communications	
4	**Security Responsibilities**	1.0
4.1	Contracting governments	
4.2	The company	
4.3	The vessel	
4.4	The port facility	
4.5	Vessel Security Officer	
4.6	Company Security Officer	
4.7	Facility Security Officer	

Subject Area			Hours
	4.8	Vessel personnel with specific security duties	
	4.9	Facility personnel with specific security duties	
	4.10	Other personnel	
5	**Vessel and Facility Security Planning**		1.0
	5.1	Methodology of vessel and port facility security assessment	
	5.2	Methods of vessel and port facility security surveys	
	5.3	Methods of conducting inspections, control, and monitoring	
	5.4	Security aspects of vessel and facility layout	
	5.5	The Vessel Security Plan, Facility Security Plan, and related procedures	
6	**Emergency Preparedness**		2.0
	6.1	Emergency preparedness, emergency response, and contingency planning	
	6.2	Crisis management	
	6.3	Security drills and exercises	
	6.4	Crowd management and control techniques	
7	**Threat Identification, Recognition, and Response**		3.0
	7.1	Maritime intelligence gathering and dissemination	
	7.2	Meaning and consequential requirements of different security levels	
	7.3	Methods of physical searches and non-intrusive inspections	
	7.4	Recognition and detection of weapons, dangerous substances and devices	
	7.5	Recognition, on a non-discriminatory basis, of persons posing potential security risks	
	7.6	Techniques used to circumvent security measures	

8	**Security Equipment**	1.0
	8.1 Security equipment and systems	
	8.2 Operational limitations of security equipment and systems	
		1.0
9	**Security Administration**	
	9.1 Documentation and records	
	9.2 Reporting security incidents	
	Total:	**15.0**

Military, First Responder, and Law Enforcement Personnel
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 Competencies to be achieved 1.3 Historical perspective 1.4 Current threats **2 Maritime, Intermodal and Supply Chain Conditions and Operations** 2.1 Maritime orientation and definitions	2.2 Supply chain and intermodal transportation system structure and operations 2.3 Port and transportation information and tracking systems 2.4 Cargo and transportation documentation	2.5 Hazardous materials security 2.6 Port and maritime security measures **3 Maritime Security Policy** 3.1 Relevant international conventions, codes, and recommendations 3.2 Relevant government legislation and regulations 3.3 Definitions 3.4 Legal implications of action or non-action by security personnel 3.5 Handling sensitive security-related information and communications	**4 Security Responsibilities** 4.1 Contracting governments 4.2 The company 4.3 The vessel 4.4 The port facility 4.5 Vessel Security Officer 4.6 Company Security Officer 4.7 Facility Security Officer 4.8 Vessel personnel with specific security duties 4.9 Facility personnel with specific security duties 4.10 Other personnel **5 Vessel and Facility Security Planning** 5.1 Methodology of vessel and port facility security assessment 5.2 Methods of vessel and port facility security surveys 5.3 Methods of conducting, inspection, control and monitoring 5.4 Security aspects of vessel and facility layout 5.5 The Vessel Security Plan, Facility Security Plan, and related procedures

Military, First Responder, and Law Enforcement Personnel
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 2	**6 Emergency Preparedness** 6.1 Emergency preparedness, emergency response, and contingency planning 6.2 Crisis management 6.3 Security drills and exercises 6.4 Crowd management and control techniques	**7 Threat Identification, Recognition and Response** 7.1 Maritime intelligence gathering and dissemination 7.2 Meaning and consequential requirements of different security levels 7.3 Methods of physical searches and non-intrusive inspections 7.4 Recognition and detection of weapons, dangerous substances and devices	7.5 Recognition of persons posing potential security risks 7.6 Techniques used to circumvent security measures **8 Security Equipment** 8.1 Security equipment and systems 8.2 Operational limitations of security equipment and systems	**9 Security Administration** 9.1 Documentation and records 9.2 Reporting security incidents Examination/Assessment

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 (1.5 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 port and maritime transportation industry, such as:

.1 piracy and armed attacks

.2 terrorism

.3 contraband smuggling

.4 stowaways and refugees

.5 cargo theft

.6 collateral damage

.7 organized crime

.8 internal conspiracies

.9 labor disputes

.10 workplace violence

.11 bombings

2 **Maritime, Intermodal, and Supply Chain Conditions and Operations** (3.5 hours)

2.1. Maritime orientation and definitions

.1 summarizes important terms used in port and maritime operations

.2 describes key industry operating practices, structure, and equipment

2.2. Supply chain and intermodal transportation system structure and operations

.1 describes key components of intermodal supply chains

2.3. Port and transportation information and tracking systems

.1 summarizes the role of information in transportation systems

.2 describes the principal identification, location, and tracking technologies in use

2.4. Cargo and transportation documentation
.1 lists the key forms of documentation used in maritime and intermodal operations
2.5. Hazardous materials security
.1 Summarizes regulatory requirements, safe operating practice, and special security considerations in the transportation and storage of HAZMAT cargoes
2.6. Port and maritime security measures
.1 lists the security measures and procedures at the three security levels required to:
.1 ensure the performance of all vessel and facility security duties
.2 control access to the vessel and facility
.3 monitor waters surrounding the vessel
.4 control the embarkation of persons and their effects aboard vessels
.5 monitor restricted areas to ensure only authorized persons have access
.6 control the handling of cargo and delivery of vessel's stores
.7 ensure the screening of unaccompanied baggage; and
.8 ensure that security communication is readily available
.9 monitor the security of the facility and its nearby approaches
.10 monitor deck areas and areas surrounding the vessel

3 **Maritime Security Policy** (1.0 hours)
3.1. Relevant international conventions, codes, and recommendations
.1 lists previous efforts of IMO, ILO, etc., towards enhanced maritime security
.2 describes 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
3.2. Relevant government legislation and regulations
.1 states the requirements of relevant legislation and regulations
3.3. Definitions
.1 defines
.1 Vessel Security Plan
.2 Company Security Officer
.3 Vessel Security Officer
.4 Port facility
.5 Vessel-to-facility interface
.6 Vessel-to-port interface
.7 Vessel-to-vessel activity
.8 Facility Security Officer
.9 Designated Authority
.10 Recognized Security Organization
.11 Declaration of Security
.12 Security incident
.13 Security Level
.14 the three security levels

.15 other important related terms

3.4 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

3.5 Handling sensitive security-related information and communications

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

4 **Security Responsibilities** (1.0 hours)

4.1. Contracting governments

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

4.2. The company

.1 notes 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

4.3. The vessel

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

4.4. The facility

.1 notes 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 notes that the facility shall act upon the security levels set by the Administration

4.5. Vessel Security Officer

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

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

4.6. Company Security Officer

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

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

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

4.7. Facility Security Officer

.1 notes that the Facility Security Officer shall be designated for each facility

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

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

4.8. Vessel personnel with specific security duties

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

4.9. Facility personnel with specific security duties

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

4.10. Other personnel

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

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

5 Vessel and Facility Security Planning (1.0 hours)

5.1 Methodology of vessel and port facility security assessment

.1 states the role of risk-based decision making in completing a security assessment

.2 describes the recommended methodology for risk assessment

.3 explains and demonstrates how to carry out an initial risk assessment

.4 identifies the types of weaknesses that may be found in the initial risk assessment

.5 summarizes the use of software and checklists in conducting security assessments

5.2 Methods of vessel and facility 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 and 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 aboard vessels and in facilities

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

.7 discusses the components and operations of systems to protect vessel and 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 vessel and facility operations and in maintaining security

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

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

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

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

.14 summarizes the identification and evaluation of facilities, transportation infrastructure, and assets

.15 summarizes the identification and evaluation of utilities and related systems

5.3 Methods of conducting inspection, control and monitoring

.1 summarizes the requirements for carrying out inspections

.2 states the requirements to review Vessel Security and Facility Security Plans as appropriate

5.4 Security aspects of vessel and facility layout

.1 summarizes the security aspects of different types of vessel layout

.2 summarizes the security aspects of different types of facility layout

5.5 The Vessel Security Plan, Facility Security Plan, and related procedures

.1 Purpose of the Vessel and Facility Security Plan

.1.1 states that each affected vessel and facility shall develop and maintain, respectively, a Vessel Security Plan and a Facility Security Plan approved by the Administration

.1.2 summarizes that the Vessel and Facility Security Plans address the security measures that should be taken at each security level

.2 Contents of the Vessel and Facility Security Plans

.2.1 summarizes the required elements of Vessel and Facility Security Plans

.2.2 states that the Vessel and Facility Security Plans shall establish procedures for the performance of vessel and facility security duties

.3 Explains Confidentiality issues

.3.1 states that the Facility Security Plan is generally confidential

.3.2 states that the Vessel Security Plan is confidential

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

.3.4 states the circumstances under which certain sections of the Vessel Security Plan may be shown to Port State Control Authorities

.4 Development of Vessel and Facility Security Plans

.4.1 states that Vessel and Facility Security Officers are responsible for ensuring that Vessel and Facility Security Plans, respectively, are prepared and submitted for approval.

.4.2 summarizes the process that should be used in development of the Vessel and Facility Security Plans.

.4.3 states that the security measures included in the Vessel or Facility Security Plan must be in place when initial verification of the plan is being carried out.

.5 Approval of Vessel and Facility Security Plans

.5.1 summarizes that all Vessel and Facility Security Plans must be approved and that if any security equipment fails or if a security measure is suspended, equivalent temporary security measures should be adopted and communicated to the Administration

.5.2 summarizes mechanisms and procedures for obtaining approval of Vessel and Facility Security Plans

.5.3 states that the Vessel Security Plan, or amendments to a previously approved plan, submitted for approval shall be accompanied by the Vessel Security Assessment on which the plan or amendments have been based

.6 Implementation of Vessel and Facility Security Plans

.6.1 summarizes procedures to be employed in implementing the Vessel and Facility Security Plans

.6.2 summarizes the requirement to ensure effective communication and cooperation between the Vessel Security Officer, the Company Security Officer, and the Facility Security Officer in the implementation of the Vessel and Facility Security Plans

.6.3 summarizes the importance of giving due regard to the effect that vessel and/or facility security measures may have on shipboard personnel who may remain on board a ship for long periods

.7 Maintenance and modification of the Vessel and Facility Security Plan

.7.1 summarizes mechanisms for ensuring the continuing effectiveness and updating of the Vessel and Facility Security Plans

.7.2 summarizes the requirement to ensure effective communication and cooperation between the Vessel Security Officer, the Company Security Officer, and the Facility Security Officer in the implementation of the Vessel and Facility Security Plans

.7.3 notes that amendments to the Vessel and Facility Security Plans shall not be implemented unless approved by the Administration

6 Emergency Preparedness (2.0 hours)

6.1 Emergency preparedness, emergency response, and contingency planning

.1 Describes emergency preparedness procedures unique to facilities, organizations and communities near or in ports and other transportation infrastructure

.2 Describes the contents of an emergency response plan of action to prevent the loss of life and minimize injury and property damage unique to facilities, organizations and communities near or in ports and other transportation infrastructure

.2.1 Lists local, state and federal agencies responsible for emergency response in marine environments and the Incident Command System structure

.2.2 discusses elements of planning for possible incidents, such as:

- Use of chemical, biological, radiological, nuclear or explosive weapons at or near a port facility or transportation infrastructure, or aboard or near a vessel, or underwater
- Vessel hijacking
- threats (chemical, biological, radiological, nuclear, explosive/bomb) near a port facility and/or aboard or near a vessel
- unidentified objects / explosives on vessel
- anti-ship mines and underwater attacker/diver capabilities
- unidentified objects / explosives at or near a port facility or transportation infrastructure
- damage to / destruction of facility and/or vessel
- piracy and other depredations
- stowaways

.3 describes contingency plans or the alternative methods to be used to respond to a disruption in services caused by a failure or emergency situations

6.2 Crisis management

.1 describes overall coordination necessary for effective response and recovery

.2 lists roles and responsibilities of members of the crisis management team

6.3 Security drills and exercises

.1 explains the purpose and procedures of drills and exercises

.2 states the requirements for conducting drills and exercises

.3 states the individual elements that each drill should test

.4 states the number and type of organizations and personnel involved in the drills

6.4 Crowd management and control techniques

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

.2 describes strategies for managing a crowd through the crisis phases

.3 summarizes the importance of clear communication with vessel crew members, passengers, facility personnel, and others during an emergency

7 Threat Identification, Recognition and Response (3.0 hours)

7.1 Maritime intelligence gathering and dissemination

.1 describes the process of maritime intelligence gathering and dissemination

.1.2 lists intelligence resources

.2 states that maritime intelligence is confidential and lists measures to ensure confidentiality

7.2 Meaning and consequential requirements of different security levels

.2 explains the three security levels and the actions required for each level

7.3 Methods of physical searches and non-intrusive inspections

.1 demonstrates how to carry out physical searches and non-intrusive inspections near and aboard vessels and in facilities

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

7.4 Recognition and detection of weapons, dangerous substances and devices

.1 demonstrates how to identify various types of weapons, dangerous substances and devices, the damage they can cause, and their appearance

.2 demonstrates how to respond to and contain weapons, dangerous substances and devices

7.5 Recognition of persons posing potential security risks

.1 summarizes 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

7.6 Techniques used to circumvent security measures

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

8 Security Equipment (1.0 hours)

8.1 Security equipment and systems

.1 demonstrates familiarity with the various types of security equipment and systems that can be used aboard vessels, in facilities, and in transportation systems

.2 Describes systems integration of security equipment

8.2 Operational limitations of security equipment and systems

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

9 Security Administration (1.0 hours)

9.1 Documentation and records

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

.2 summarizes the Statement of Compliance of a Facility, its validity and verification requirements

.3 summarizes the International Ship Security Certificate, its validity and verification requirements

.4 summarizes the requirements of the vessel Continuous Synopsis Record and what it shall contain

.5 summarizes the activities for which records shall be kept and the duration for which they should be retained

9.2 Reporting security incidents

.1 states the reporting requirements in case of a security incident or a breach of security

Total: 15.0 hours

Part D: Instructor Manual

The instructor manual provides guidance on the material that is to be presented during the course for military, first responder, and law enforcement personnel working in the maritime domain. This manual reflects the views of the course developers and expert reviewers with respect to methodology and organization as well as what they consider relevant and important in light of their experience. 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. Each instructor will need to adjust the presentation of material to account for the varying rank, legal authority, and jurisdiction of military, first responder, and law enforcement personnel taking the course.

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

1. Introduction
2. Maritime, Intermodal and Supply Chain Conditions and Operations
3. Maritime Security Policy
4. Security Responsibilities
5. Vessel and Facility Security Planning
6. Emergency Preparedness
7. Threat Identification and Recognition
8. Security Equipment
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 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 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 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 military, first responder, and law enforcement 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 occurs on 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 tactics.

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 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. 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.

2 Maritime, Intermodal, and Supply Chain Conditions and Operations

This section of the course should provide trainees with an understanding of the larger context in which maritime, intermodal and supply chain operations occur. Understanding the complex transportation and logistics framework of the maritime system will enable students to effectively undertake their security responsibilities. Familiarity with key definitions, terminology, and operational practices employed in the maritime realm is important for military, first responder, and law enforcement personnel who may be called upon to function in this environment. 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.

2.1 Maritime orientation and definitions

Trainees should be provided with an orientation to key terms and operational practices in the marine transportation system. Appropriate topics in this familiarization include basic nautical terminology, vessel types and construction, port and terminal operating practices, equipment and technology, steamship company organization, cargo types and methods of shipment, and related subjects.

2.2 Supply chain and intermodal transportation system structure and operations

The objective of this segment of the course should be to develop student awareness of the key components and parties involved in the movement and storage of goods from source of raw materials to end user. Trainees should be made aware of the interaction and interfaces between modes of transportation and the sequence of events characterizing the typical movement of intermodal containers, with particular focus on opportunities for criminal activity at each juncture.

2.3 Port and transportation information and tracking systems

This segment should focus on the role of information in the movement of ships, trucks, trains, containers, and other elements of port and intermodal transportation systems. Vessel and cargo identification and location system approaches and technologies should be explained. Vessel traffic systems, yard management systems, container tagging and tracking systems, and related information systems should be described.

2.4 Cargo and transportation documentation

The various forms of documentation pertaining to the operation of vessels, vehicles, and terminals, and the movement of cargo and passengers should be summarized for trainees. The bill of lading, cargo manifest, and crew list are examples of the type of documentation with which students should be familiar.

2.5 Hazardous materials security

Trainees should become familiar with the specific operational considerations and regulatory requirements that are associated with the movement and storage of HAZMAT cargoes. DOT regulations on hazardous materials shipping; segregation of reactive materials aboard ships and in terminals; requirements of the IMDG Code; regulations concerning labelling and placarding; transportation of hazardous waste, and related issues should be discussed.

2.6 Port and maritime security measures

Trainees should be made aware of security procedures for which vessel and facility personnel are responsible, such as security inspections, controlling access to the vessel and facility, monitoring deck areas and areas surrounding the ship, screening of unaccompanied baggage, and so forth.

3 Maritime Security Policy

3.1 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 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 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.

3.2 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.

3.3 Definitions

Trainees will need a working knowledge of terms found in 33 CFR Subchapter H, SOLAS Chapter XI-2 Regulation 1, in the ISPS Code Part A section 2, etc. For instance, it might require clarification by the instructor to establish that the Vessel Security Officer is a person on board the ship and in that sense it may be impossible for a Company Security Officer to also act as the Vessel Security Officer. The instructor should provide written reference material on the various regulatory definitions, including:

1. Vessel Security Plan
2. Company Security Officer
3. Vessel Security Officer
4. Port facility
5. Vessel-to-facility interface
6. Vessel-to-port interface
7. Vessel-to-vessel activity
8. Facility Security Officer
9. Designated Authority
10. Recognized Security Organization
11. Declaration of Security
12. Security incident
13. Security Level
14. the three security levels

3.4 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.

3.5 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 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.

4 Security Responsibilities

This section is intended to give trainees a clear picture of the proportions of the maritime security system and to show how various entities will work together to form an efficient and effective whole. These entities include local, state, federal law enforcement agencies, military, other government agencies, contracting governments, Recognized Security Organizations, the company, the vessel and the (port) facility.

4.1. Contracting governments

Instructors should discuss the roles of contracting governments and their obligations in the international scheme to enhance maritime security. An awareness 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.

4.2. 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.

4.3. 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 be aware of the requirements relating to the security of the vessel in its role as the cornerstone of the marine transportation system.

4.4. The port 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.

4.5- 4.10 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 appreciate 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.

5 Vessel and Facility Security Planning

5.1 Methodology of vessel and port facility security assessment

Vessel and facility security assessments are an essential and integral part of the process of developing, updating and inspecting Vessel and Facility Security Plans. In this segment of the course, it should be communicated to trainees that risk-based decision-making is one of the best tools to complete a security assessment and to determine appropriate security measures for vessels and facilities. 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 of vessels and facilities is provided in the ISPS Code Part B.

Trainees in port facility environments can benefit from knowing that the Facility Security Officer may delegate the assessment to a person(s) with skills to evaluate the security of a facility and carry out the Facility Security Assessment. They should also know that the Facility Security Assessment may be conducted by a Recognized Security Organization - or private security contractor - but that approval of a completed Facility Security Assessment should only be given by the U.S. Coast Guard.

Trainees should be instructed that, prior to commencing or evaluating a Facility Security Assessment, those responsible should obtain current information on the assessed threat for the local area and should be knowledgeable about the types of vessels calling on the facility. The officer should identify and evaluate possible threats to key facility operations, assets and infrastructure, and the likelihood of their occurrence, in order to establish and prioritize security measures. Understanding of the local port operations is vital as the nature of these operations will determine the types of threats the port is exposed to and in turn, the vulnerabilities specific to each threat.

The trainee should study previous reports on similar security requirements. The trainee should know that when feasible, he or she should consult with appropriate port personnel and other Facility Security Officers on the methodology and aspects of the assessment. The trainee should know to examine access points, including rail access, roads, waterside, and gates, and evaluate their potential for use by unauthorized individuals who may cause transportation security incidents. This includes individuals with legitimate access as well as those who seek to obtain unauthorized entry.

5.2 Methods of vessel and port facility security surveys

Trainees should understand that the vessel security surveys should fulfil the following functions:

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

It should be emphasized to course participants that the on-scene survey should examine and evaluate existing shipboard 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

- monitoring the waters surrounding the vessel for both surface and signs of subsurface activity that could place unknown persons in direct or close contact with 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's stores;
- ensuring that vessel security communication, information, and equipment are readily available; and
- Alertness to the potential for sabotage of shipboard emergency systems including fire detection, response and suppression.

It should be imparted to trainees that the Facility Security Assessment should include an on-scene security assessment and evaluation of the facility, to include the following elements:

- General layout of the facility;
- 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;
- Numerical strength, reliability, and security duties of the facility's personnel;
- Security doors, barriers, and lighting;
- Location of areas which should have restricted access, such as control stations;
- Communications centres, cargo storage areas, etc.;
- Emergency and stand-by equipment available to maintain essential services;
- Response procedures for fire or other emergency conditions;
- Existing security and safety equipment for protection of personnel and visitors;
- Level of supervision of the facility's crew, vendors, repair technicians, dock workers, etc.;
- Existing agreements with private security companies providing port facility security services at all security levels, including any security forces contracted by visiting vessels;
- Procedures for control of security keys and other access prevention systems;
- Cargo and vessel stores operations; and
- Response capability to incidents.

5.3 Methods of conducting inspection, control and monitoring

Trainees should understand that inspection, control and monitoring refer to the Vessel and Facility Security Plans themselves. Inspections, control and monitoring should be conducted to formally assess the effectiveness of all aspects of Vessel and Facility Security Plans. 33 CFR Subchapter H and the ISPS Code provide useful material for instruction in this subject.

5.4 Security aspects of vessel and facility layout

The instructor can explain vessel and facility layouts to assist trainees in developing the ability to identify potential vulnerabilities and anomalies and evaluate appropriate emergency response options and search techniques. Trainees can benefit from understanding key differences between the various types of vessels as well as facilities.

5.5 The Vessel Security Plan, Facility Security Plan, and related procedures

The instructor should summarize the main requirements of the Vessel and Facility Security Plans and procedures to implement them. The trainees can benefit from being aware of the Vessel and Facility Security Plans purpose, contents, development, approval process, implementation as well as maintenance and modification. The instructor should stress how confidentiality for vessels is higher than for facilities for appropriate military, first responder, and law enforcement personnel.

6 Emergency Preparedness

6.1 Emergency preparedness, emergency response, and contingency planning

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. Appropriate action to be taken in the case of bomb threats, explosions, piracy, hijackings, and similar events should be discussed in terms of the Incident Command System. Although military, first responder, and law enforcement trainees are trained and familiar with emergency preparedness, emergency response and contingency planning; trainees must learn key differences between land- and marine-side requirements.

6.2 Crisis management

The instructor should give the trainees a detailed description of the broad overall coordination of a security breach using the Incident Command System, particularly given the wide variety of local, state and federal agencies that can be involved in a maritime-related event.

6.3 Security drills and exercises

It should be conveyed to course participants that the objective of drills and exercises is to ensure that vessel and facility personnel are proficient in all assigned security duties at all security levels and in the identification of any security related deficiencies, which 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 that have not previously participated in any drill on that vessel within the last 3 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 of a port 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 vessel 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 involving participation of vessel 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.

6.4 Crowd management and control techniques

Course participants should be familiarized with the basic patterns of behaviour of people in groups during time of crisis. Basic techniques that can be employed in attempts to control crowds in the case of a security incident or threat should be communicated to participants. The critical importance of clear communication with vessel personnel, port facility personnel, passengers, and others involved should be underscored.

7 Threat Identification, Recognition and Response

7.1 Maritime intelligence gathering and dissemination

The instructor should explain the process of collecting and prioritizing intelligence to explain how information and/or incidents are determined to require action. Trainees should be aware of the resources

available to them, such as government classified and unclassified reports, information and notification from Port State Control, public-private sector partnerships and open-source information. The instructor should reinforce the importance of confidentiality and give examples of circumstances when to release intelligence in seeking assistance from vessel or facility security personnel.

7.2 Meaning and consequential requirements of different security levels

The instructor should convey the different types of security measures that should be considered for ships at sea and those in port as well as facilities as they respond to security incidents and security levels 1, 2 and 3. Feedback from or discussion among the trainees will help in deciding whether or not the necessary knowledge is being conveyed. Trainees may benefit from an in-class creation of a checklist detailing the appropriate generic actions given various conditions.

7.3 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 vessels, persons, personal effects, baggage, cargo, container yards, terminals, vessel stores, and other areas and items of concern. Trainees should be informed that, unless there are clear security grounds for doing so; members of a vessel's crew or 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.

7.4 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. The instructor should focus on issues unique to the port and maritime environment.

Recognition training should include basic instruction for the recognition of military weapons, ammunition and demolition components that may be used in a potential attack scenario, or could be the subject of smuggling efforts connected with terrorism. Foreign military explosives and explosive munitions can take many forms and may often be overlooked, or appear as objects that do not signal an immediate threat.

7.5 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
- The appearance of uniformed seamen or officers who are attempting to enter facilities or board vessels without full authentication
- 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
- Small boats, dhows, or similar vessels shadowing a ship and/or making probing runs at ships to check their response

7.6 Techniques used to circumvent security measures

Trainees should be reminded 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.

8 Security Equipment

8.1 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

- Binoculars, 7 x 50
- 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. However, military, first responder, and law enforcement personnel may be called upon to operate and interpret readings obtained from such equipment in the port, maritime, and intermodal environment.

8.2 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.

9 Security Administration

9.1 Documentation and records

Trainees should be aware of the required vessel and facility security documentation including the validity and verification requirements of the vessel International Ship Security Certificate and Continuous Synopsis Record as well as the Statement of Compliance of a Facility.

9.2 Reporting security incidents

Trainees should be aware of the vessel and facility personnel reporting requirements in case of a security incident or a breach of security in order to respond and/or investigate incidents accordingly. 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 documenting, sharing and/or responding to these reports.

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 percent. 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 percent chance of gaining one mark and a 75 percent chance of losing one mark.

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