



# **ABS Consulting**

**GUIDE FOR**

---

## **PORT SECURITY**

**October 2003**

**ABS Consulting**

**Copyright Ó 2003  
ABSG Consulting Inc.  
ABS Plaza  
16855 Northchase Drive  
Houston, TX 77060 USA  
E-mail: [portsecurityguide@absconsulting.com](mailto:portsecurityguide@absconsulting.com)**



## ***ACKNOWLEDGMENTS***

ABS Consulting and the authors of the *Guide for Port Security (Guide)* – Myron Casada, Thomas Nolan, David Trinker, and David Walker – are indebted to those who contributed to and reviewed the *Guide* during its development. Extracts from the International Convention for the Safety of Life at Sea (SOLAS), 1974, and the International Ship and Port Facility Security (ISPS) Code are reproduced by kind permission of the International Maritime Organization (IMO). The complete text of the ISPS Code can be purchased from IMO at its Web site [www.imo.org](http://www.imo.org).

### ***Contact Information***

ABS Consulting provides training, consulting services, and software to help our clients meet the International Convention for the Safety of Life at Sea (SOLAS), International Ship and Port Facility Security (ISPS) Code, and U.S. Coast Guard requirements. If you need to discuss maritime security issues or have questions regarding these regulations, please contact:

<b>Port Security and Training Issues</b>	<b>Fixed-facility Issues</b>
Mr. Myron Casada 865-671-5815 <a href="mailto:mcasada@absconsulting.com">mcasada@absconsulting.com</a>	Mr. Steve Arendt 865-671-5812 <a href="mailto:sarendt@absconsulting.com">sarendt@absconsulting.com</a>
<b>Ship Security and Training Issues</b>	<b>International Port Security and Training Issues</b>
Mr. Tom Nolan 281-877-5906 <a href="mailto:tnolan@absconsulting.com">tnolan@absconsulting.com</a>	Mr. David Trinker 865-671-5840 <a href="mailto:dtrinker@absconsulting.com">dtrinker@absconsulting.com</a>



## **TABLE OF CONTENTS**

<b><u>Section</u></b>	<b><u>Page</u></b>
<b>ACKNOWLEDGMENTS</b> .....	iii
<b>FOREWORD</b> .....	vii
<b>1. GENERAL</b> .....	1
1.1 Scope and Application .....	1
1.1.1 Ports Versus Port Facilities .....	1
1.2 Security Assessments .....	5
1.3 Statement of Compliance .....	6
1.3.1 General .....	6
1.3.2 Compliance Process .....	6
1.3.3 Representations .....	7
1.3.4 Termination .....	7
1.4 Limitation of Liability .....	7
1.5 Definitions .....	7
1.6 References .....	8
1.6.1 International Security Requirements .....	9
1.6.2 International and Selected Government Guidance Documents .....	9
1.6.3 Other Useful References .....	9
<b>2. MARITIME SECURITY</b> .....	11
2.1 General .....	11
2.2 Process Overview .....	11
2.3 Security Levels .....	12
2.4 Administrations .....	12
2.5 Contracting Governments .....	12
<b>3. CONTRACTING GOVERNMENT RESPONSIBILITIES</b> .....	15
3.1 Port Security Assessments .....	15
3.1.1 International Requirements .....	15
3.1.2 ABS Consulting Guidance .....	16
3.2 Verification of Compliance for Port Facilities .....	17
3.2.1 International Requirements .....	17
3.2.2 ABS Consulting Guidance .....	17
3.3 Alternative Agreements and Equivalent Requirements .....	17
3.3.1 International Requirements .....	17
3.3.2 ABS Consulting Guidance .....	18

## **TABLE OF CONTENTS (cont'd)**

<b><u>Section</u></b>	<b><u>Page</u></b>
<b>4. PORT FACILITY RESPONSIBILITIES .....</b>	<b>19</b>
4.1 Port Facility.....	19
4.1.1 International Requirements .....	19
4.1.2 ABS Consulting Guidance .....	20
4.2 Port Facility Security Officer .....	20
4.2.1 International Requirements .....	20
4.2.2 ABS Consulting Guidance .....	21
4.3 Port Facility Security Assessments.....	22
4.4 Port Facility Security Plans .....	22
4.4.1 International Requirements .....	22
4.4.2 ABS Consulting Guidance .....	24
4.5 Training and Drills .....	25
4.5.1 International Requirements .....	25
4.5.2 ABS Consulting Guidance .....	26
4.6 Security Records.....	26
4.6.1 International Requirements .....	26
4.6.2 ABS Consulting Guidance .....	26
4.7 Audits and Reviews .....	27
4.7.1 International Requirements .....	27
4.7.2 ABS Consulting Guidance .....	27
4.8 Declaration of Security.....	27
4.8.1 International Requirements .....	27
4.8.2 ABS Consulting Guidance .....	28
<b>APPENDIX 1 Guidance for Performing Port and Port Facility Security Assessments.....</b>	<b>A1-1</b>
<b>APPENDIX 2 Example Port Facility Security Plan .....</b>	<b>A2-1</b>

# ***ABS CONSULTING GUIDE FOR PORT SECURITY***

## ***FOREWORD***

In the maritime world, safety and security are closely linked. Traditionally, much of the emphasis of ABS Consulting's services has been on safety, and ABS Consulting applied its risk technology and knowledge to assist its clients in maintaining safety through prevention of accidents caused by the forces of nature and human error. While the science of those causes is complex, the causes are amenable to analysis, understanding, and prediction.

Maritime security introduces an additional element into the safety equation: deliberate actions by people intent on causing harm. Security has always been a concern with naval ships and facilities, and the military routinely exercises precautions to maintain the security of its assets. Commercial vessels and associated facilities have routinely employed special security measures under certain circumstances to prevent piracy, smuggling, or stowaways. Those crimes are usually economically motivated, where destruction is not the goal. Acts of terror are usually politically motivated, and ports and port facilities are prime targets because (1) they play a large role in international commerce, bringing together resources from many different countries, and (2) they are often in close proximity to large population centers, industrial centers, and critical infrastructure assets. Because of these characteristics, ports and port facilities present high potential for terrorists to cause extensive damage to life, property, the environment, and the transportation and economic infrastructure. The maritime community has come to the realization that ports and port facilities must be made less vulnerable to security threats, both to protect the port assets and to protect the vessels using those ports.

On December 12, 2002, during a diplomatic conference of the International Maritime Organization (IMO), Contracting Governments adopted amendments to the International Convention for the Safety of Life at Sea (SOLAS), 1974, to enhance the security of ships and port facilities. In addition to completing a new Chapter XI-2, "Special Measures to Enhance Maritime Security," the IMO diplomatic conference also approved a new International Ship and Port Facility Security Code (ISPS Code). Compliance with Part A of the ISPS Code is mandatory. Part B of the ISPS Code contains guidance for applying the new SOLAS requirements and Part A requirements of the ISPS Code. The amendments and requirements are effective as of July 1, 2004. Flag Administrations (for ships) and Contracting Governments (for port facilities) may delegate some of their responsibilities under the new security regime to Recognized Security Organizations.

ABS Consulting, one of the world's largest risk management firms, is involved in port and port facility security activities. ABS Consulting is providing services to governments and companies as they take action to meet their port and port facility security responsibilities under the ISPS Code. ABS Consulting has prepared this *Guide for Port Security (Guide)* to assist governments, companies, and individuals in applying the port security provisions of SOLAS and the ISPS Code. It is not intended as a substitute for those documents. However, when used in conjunction with SOLAS and the ISPS Code, this *Guide* may be helpful in achieving compliance with the international regulations.

*This October 2003 edition of the Guide for Port Security is being issued to assist ABS Consulting clients in developing and implementing their port and port facility security programs. The maritime security area is changing rapidly and the IMO and governmental authorities will all be revising their guidelines and adding to the resources available to help companies meet the new requirements. We welcome your feedback. Comments or suggestions can be sent electronically to portsecurityguide@absconsulting.com or faxed to ABS Consulting in the United States at (865) 966-5287.*



# ***1. GENERAL***

## ***1.1 SCOPE AND APPLICATION***

This *Guide for Port Security (Guide)* has been developed by ABS Consulting with the objective of improving security in the operation of ports and port facilities associated with ships in international service. ABS Consulting recognizes the positive impact that sound security management practices have in reducing losses to the maritime industry due to terrorism, piracy, and other criminal activity. This *Guide* provides the maritime industry with a model for implementing port and port facility security programs.

This *Guide* is intended for the use of organizations operating all types of ports and port facilities that need to meet the requirements of the International Ship and Port Facility Security (ISPS) Code developed by the International Maritime Organization (IMO). The *Guide's* requirements are stated in general terms in order to apply to a wide variety of ports and port facilities. This *Guide* addresses the basic requirements developed by the international community for application to port facilities serving ships involved in international commerce. The term “ships” used in the international regulations includes passenger ships, cargo ships over 500 gross tonnage, high speed cargo and passenger ships, and mechanically propelled mobile offshore drilling units (MODUs). This *Guide* may also be used for port facilities involving other ships, such as cargo ships less than 500 gross tonnage and ships not involved in international commerce, to improve their security programs. If requested by the port facility operator, ABS Consulting will verify and provide an ABS Statement of Compliance for the security program of any port facility in accordance with this *Guide*. The issuance of a Statement of Compliance by a Contracting Government is described in Part B (Section 16.62) of the ISPS Code. However, ABS Consulting will only provide Statements of Compliance that address the requirements of this *Guide*, unless appointed as a Recognized Security Organization for port facilities by a specific Contracting Government. In that situation, ABS Consulting would issue a Statement of Compliance that addresses the specific requirements of that Contracting Government.

### ***1.1.1 Ports Versus Port Facilities***

The ISPS Code provisions that apply to port facilities were carefully considered and debated at IMO. Typically, International Convention for the Safety of Life at Sea (SOLAS) requirements are applicable only to ships, as is appropriate for requirements to ensure safety of life at sea. However, it was recognized that a great deal of the security vulnerability for such ships is controlled by security measures that must be implemented by, or at least coordinated with, port facilities. Activities such as docking, taking on ship's stores, loading and unloading cargo, and embarking and disembarking passengers and crew involve both the ship and the port facility where those actions occur. The ISPS Code defines activities like these as the “ship/port interface.” The term “port facility” is defined as the location where the ship/port interface occurs.

The ISPS Code requirements do not address the entity that operates the port facility, only what security functions must occur and what the responsibilities of the Contracting Government (i.e., the Port State) and the port facility are. In some countries and some specific locations, the port facility will be operated by a municipal, state/provincial, or national organization; however, more often, the port facility will be operated by an industrial entity, regulated by some combination of public entities.

The ISPS Code requires that the Contracting Government perform a port facility security assessment, which, when appropriate, can address more than one port facility. It is expected

that most Contracting Governments will perform these assessments themselves or contract with a consulting firm to provide the assessments on a portwide basis.

For example, in the United States, the federal authority for maritime safety and security at the port level resides with the U.S. Coast Guard (USCG) Captains of the Port (COTPs). Most waterside facilities that interface with ships are operated either by port authorities chartered by state or local governments or by industrial corporations/companies. To implement the IMO maritime security requirements in the United States, the USCG has developed interim final regulations, which were published in the *U.S. Federal Register* on July 1, 2003. Those regulations require that the COTPs, in conjunction with port security committees, perform port security assessments and develop the security plans required by the ISPS Code for “port facilities.” Also, the USCG regulations define which facilities must develop lower-level “facility” plans and perform security assessments. Table 1 provides a cross reference between the USCG regulation related to port facilities (i.e., 33 CFR Part 105) and the corresponding portions of the ISPS Code. It is provided to help the reader understand how the USCG regulation addresses the ISPS Code requirements.

**Table 1 Cross Reference Between the USCG Maritime Facility Security Regulation (33 CFR Part 105) and the Pertinent Sections of the ISPS Code**

USCG Requirements		Corresponding ISPS Code Section	
Part 105	Topic	PART A	PART B
<b>Subpart A</b>	<b>General</b>		
105.100	Definitions	Section 2	Section 2
105.105	Applicability	Section 3	Section 3
105.106	Public access areas	N/A	N/A
105.110	Exemptions	N/A	N/A
105.115	Compliance dates	Resolution (see Note 1)	Resolution (see Note 1)
105.120	Compliance documentation	N/A	Section 16.62
105.125	Noncompliance	N/A	
105.130	Waivers	N/A	N/A
105.135	Equivalents	N/A	Section 4.27
105.140	Alternative Security Program	N/A	N/A
105.145	Maritime Security (MARSEC) Directive	Section 4	Section 4.13
105.150	Right to appeal	N/A	N/A
<b>Subpart B</b>	<b>Facility Security Requirements</b>		
105.200	Owner or operator	N/A	N/A
105.205	Facility Security Officer (FSO)	Section 17	Section 17
105.210	Facility personnel with security duties	Section 18.2	Section 18.2
105.215	Security training for all other facility personnel	Section 18	Section 18.3
105.220	Drill and exercise requirements	Section 18.3	Section 18.4,18.5,18.6
105.225	Facility recordkeeping requirements	Section 17	N/A
105.230	Maritime Security (MARSEC) Level coordination and implementation	Section 14	N/A

**Table 1 Cross Reference Between the USCG Maritime Facility Security Regulation (33 CFR Part 105) and the Pertinent Sections of the ISPS Code (cont'd)**

USCG Requirements		Corresponding ISPS Code Section	
Part 105	Topic	PART A	PART B
105.235	Communications	Section 14.2.7	Section 16.8.4
105.240	Procedures for interfacing with vessels	Section 16.3.74	Section 16.8.4
105.245	Declaration of Security (DoS)	Section 5	Section 5
105.250	Security systems and equipment maintenance	Section 17.2.12	Section 16.8.7
105.255	Security measures for access control	Section 14	Section 16.10 - 16.20
105.260	Security measures for restricted areas	Section 14	Section 16.21 - 16.29
105.265	Security measures for handling cargo	Section 14	Section 16.30 - 16.37
105.270	Security measures for delivery of vessel stores and bunkers	Section 14	Section 16.38 - 16.44
105.275	Security measures for monitoring	Section 14	Section 16.49 - 16.54
105.280	Security incident procedures	Section 16.3.3	Section 16.8
105.285	Additional requirements - passengers and ferry facilities	N/A	N/A
105.290	Additional requirements - cruise ship terminal	N/A	N/A
105.295	Additional requirements - certain Dangerous Cargo (CDC) facilities	N/A	N/A
105.296	Additional requirements - barge fleeting facilities	N/A	N/A
<b>Subpart C</b>	<b>Facility Security Assessment (FSA)</b>		
105.300	General	Section 15	Section 15.1,15.2
105.305	FSA requirements	Section 15	Section 15.3 - 15.16
105.310	Submission requirements	Section 15	Section 15.1,15.2
<b>Subpart D</b>	<b>Facility Security Plan (FSP)</b>		
105.400	General	Section 16.1	Section 16.1
105.405	Format and content of the FSP	Section 16	Section 16
105.410	Submission and approval	Section 16	Section 16.61
105.415	Amendment and audit	Section 16	Section 16.58,16.59,16.60

Note 1: Compliance dates for the ISPS Code are provided in Resolution 1 of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974, Adopted on December 12, 2002. It is entitled “Adoption of Amendments to the Annex to the International Convention for the Safety of Life at Sea, 1974.”

Much of the USCG approach for security was outlined in 2002 in a series of Navigation and Vessel Inspection Circulars (NVICs) that provide guidance to be used in conjunction with the regulations. The security-related NVICs are:

- NVIC 4-02, *Security for Passenger Vessels and Passenger Terminals*, April 2002
- NVIC 9-02, *Guidelines for Port Security Committees and Port Security Plans Required for U.S. Ports*, September 2002

- NVIC 10-02, *Security Guidelines for Vessels*, October 2002
- NVIC 11-02, *Recommended Security Guidelines for Facilities*, January 2003

Table 2, which is adopted from Table 4 in the preamble to the USCG interim (July 1, 2003) final regulations, shows the structure of the ISPS Code requirements, as well as the documents and people addressed in the USCG regulations and guidance documents, that are needed to meet those requirements.

**Table 2 Comparison of ISPS Code and USCG Regulations/Guidance**

ISPS Code	USCG Interim Regulations	USCG Guidance (NVIC)
<b>Assessments</b>		
Port Facility Security Assessment	Area Maritime Security Assessment (33 CFR 103.400)	Port Security Assessment (NVIC 9-02)
Ship Security Assessment	Vessel Security Assessment (33 CFR 104.300)	Vessel Security Assessment (NVIC 10-02)
None	Facility Security Assessment (33 CFR 105.300)	Facility Security Assessment (NVIC 11-02)
<b>Plans</b>		
Port Facility Security Plan	Area Maritime Security Plan (33 CFR 103.500)	Port Security Plan (NVIC 9-02)
Ship Security Plan	Vessel Security Plan (33 CFR 104.400)	Vessel Security Plan (NVIC 10-02)
None	Facility Security Plan (33CFR105.400)	Facility Security Plan (NVIC 11-02)
<b>People/Positions</b>		
Port Facility Security Officer (PFSO)	Captain of the Port	Captain of the Port
Company Security Officer	Company Security Officer	Company Security Officer
Ship Security Officer	Vessel Security Officer	Vessel Security Officer
None	Facility Security Officer	Facility Security Officer
None	Area Maritime Security Committee	Port Security Committee

How other Contracting Governments will implement the ISPS Code is not as well understood. Many of them will implement a process much like the USCG approach, but have not yet published guidance, nor have they started regulatory actions. In this *Guide*, we assume that authorities for other Contracting Governments will follow a similar multi-tiered approach. However, ABS Consulting will work with governmental authorities and port facilities as required to help them define approaches for port security assessments and plans that meet both the ISPS Code and national/local regulations and requirements. For clarity, throughout this *Guide*, we use the term “port” when we are talking about the overall port and the term “port facility” when we are speaking of individual facilities where ship/port interfaces occur. However, we have not modified the SOLAS and ISPS Code terminology when we present material taken from those documents. They use the term “port facility” almost exclusively.

The requirements of this *Guide* have been largely derived from the requirements prepared by the IMO and adopted at its diplomatic conference in December 2002. Those requirements consist of changes to the SOLAS 74, including:

- SOLAS Chapter XI-2, “Special Measures to Enhance Maritime Security”
- International Ship and Port Facility Security Code (ISPS Code), Part A, Mandatory Requirements
- International Ship and Port Facility Security Code (ISPS Code), Part B, Guidance

The full text of each of these international requirements is available from IMO at its Web site [www.imo.org](http://www.imo.org). Also, for port operators who are concerned with ensuring that their activities satisfy the USCG requirements, the interim final regulations on maritime security published by the USCG on July 1, 2003, are available on ABS Consulting's Web site. Those regulations apply until they are superceded by final regulations expected in November 2003.

The ISPS Code has two parts: Part A contains the mandatory provisions of the ISPS Code, and Part B contains additional recommendations and guidance. This *Guide* incorporates some of the recommendations in Part B of the ISPS Code and other references on port facility security that ABS Consulting believes are necessary for an effective security program. Those references are listed in Section 1.6 of this *Guide*, and they include requirements and guidance published by the USCG for port facilities in the United States. The requirements and guidance developed by the USCG may also be valuable for non-U.S. port facilities that handle ships, cargo, or passengers bound for U.S. destinations. Also, the USCG and the European Commission have both indicated that they intend to make portions of Part B of the ISPS Code mandatory. If ABS Consulting is acting for a national authority, it will follow the regulations and guidance established by that government. If acting solely on the part of a port facility that wants assistance, ABS Consulting will use the requirements of this *Guide* or other specific requirements defined by the contract under which the work is authorized.

Although this *Guide* has been developed principally to address international port and port facility security requirements, some maritime safety issues are also addressed. Security requirements cannot be allowed to place a ship and crew or personnel in a port facility in an intolerable safety situation. It is necessary to examine security requirements as they are developed and improved in order to ensure they do not violate the basic requirements for safety at sea and in port facilities associated with the ship/port interface.

This *Guide* is subject to review and revision. Updates shall include, among other things, additional requirements or clarification of existing requirements. Port facilities that have received a Statement of Compliance based on the requirements of this *Guide* shall be required to comply with those changes at the next intermediate verification that occurs at least a year after publication of the changes. If the *Guide* changes are based on changes to the international or national security requirements, the applicable compliance dates of those requirements will apply.

## **1.2 SECURITY ASSESSMENTS**

In Part A of the ISPS Code (Section 15), Contracting Governments are tasked with the responsibility to perform Port Facility Security Assessments. They can delegate that responsibility to an appropriately qualified Recognized Security Organization (RSO), but must retain the responsibility for review and approval of any port facility security assessments. The USCG has defined how Port and Port Facility Security Assessments will be performed, and ABS Consulting can assist port facilities in meeting those requirements. For other Contracting Governments, ABS Consulting will work with a port facility operator to define an assessment process that will satisfy the ISPS Code; however, the port facility operator will be responsible for working with ABS Consulting for defining an approach that meets the needs of, and will satisfy, the appropriate Contracting Government(s) and Flag Administration(s) (i.e., for ships that will use that port facility).

### **1.3 STATEMENT OF COMPLIANCE**

#### **1.3.1 General**

Port facility operators may choose to implement security measures suitable to their organization's goals, objectives, and concerns. ABS Consulting encourages all companies to use this *Guide* as an aid in implementing the ISPS Code for ports and port facilities. However, to obtain a "Statement of Compliance" as defined in Part B (Section 16.62) of the ISPS Code, the port facility operator must implement a Port Facility Security Plan approved by the appropriate Contracting Government.

When a Contracting Government appoints ABS Consulting to review and provide Statements of Compliance for Port Facility Security Plans, ABS Consulting will issue the statement on behalf of that government, once the verification actions defined in this *Guide* and any applicable national regulations have been satisfied. However, approval of a Port Facility Security Plan can be provided only by a Contracting Government. As a consulting firm, or even in those situations where a Contracting Government authorizes ABS Consulting to provide services as a Recognized Security Organization, ABS Consulting cannot "approve" Port Facility Security Plans. ABS Consulting will work with its clients and Contracting Governments to meet any national requirements to achieve government approval; however, obtaining approval of a Port Facility Security Plan by the applicable government is the responsibility of the port facility operator. ABS Consulting will work with port facility operators to identify any additional requirements, beyond those contained in this *Guide*, applicable to ports and port facilities in a specific national authority region. Those additional requirements must be satisfied in order for ABS Consulting to issue a Statement of Compliance that addresses all of the identified requirements to obtain national approval of the Port Facility Security Plan.

A port facility assessed by ABS Consulting and found to meet the requirements specified in this *Guide* is entitled to hold a corresponding Statement of Compliance issued by ABS Consulting. All such statements are subject to periodic and intermediate verifications as defined in this *Guide* or by national authorities. Statements of Compliance are nontransferable. Verifications of compliance are based upon a sampling process. The absence of recorded nonconformities does not mean that none exist.

Nothing contained herein or in any document issued in connection with a Statement of Compliance is intended to relieve the owner or operator of any port or port facility from its duty to provide and ensure compliance with the appropriate regulations, or to relieve any designer, builder, owner, manufacturer, seller, supplier, repairer, operator, insurer, or other entity of any duty to inspect, or any duty or warranty, express or implied, or to create any interest, right, claim, or benefit in any insurer or other third party and such document does not create any interest, right, claim, or benefit to any third party.

#### **1.3.2 Compliance Process**

Companies seeking a Statement of Compliance with the requirements of this *Guide* for their port facilities shall fulfill the following responsibilities, some of which are more fully described in subsequent sections of this *Guide*:

- Document, implement, and maintain a Port Facility Security Plan in accordance with the requirements of this *Guide*.
- As directed by the Contracting Government, submit the plan to the appropriate authority and take whatever actions are directed by that authority to obtain approval of that plan.
- Provide ABS Consulting copies of the approved Port Facility Security Plan and the associated Port Facility Security Assessment documentation.

- Allow ABS Consulting access during normal working hours to port facilities requiring verification in order to verify compliance with the approved security plan, verify security systems/equipment, and evaluate compliance with the requirements of this *Guide*.

### **1.3.3 Representations**

A Statement of Compliance is a representation by ABS Consulting that, at the time of verification, the port facility had established and implemented a security program in accordance with the security plan approved by the appropriate Contracting Government. Any noncompliant condition that has developed or manifested itself subsequent to the most recent review and statement will not be reflected in the review or statement. A Statement of Compliance is not a representation that the port facility owner or operating Company always acts in compliance with the security plan or that the security plan addresses all contingencies. Compliance with all applicable requirements remains the responsibility of the port or port facility operator.

### **1.3.4 Termination**

The continuance of a Statement of Compliance is conditional upon the port facility's continued compliance with the requirements of this *Guide*. ABS Consulting reserves the right to reconsider, withhold, suspend, or cancel a Statement of Compliance for noncompliance with the requirements, refusing access to the port facility for verification purposes, or nonpayment of fees that are due on account of services related to obtaining the Statement of Compliance.

## **1.4 LIMITATION OF LIABILITY**

ABS Consulting shall not be liable or responsible in any respect for any inaccuracy or omission in this *Guide* or any other publication or document issued by ABS Consulting related to this *Guide*. The combined liability of ABS Consulting, its officers, directors, employees, agents, and subcontractors for any loss, claim, or damage arising from negligent performance or nonperformance of any of its services, or from breach of any implied or express warranty of workman-like performance in connection with those services, or from any other reason, to any other person, corporation, partnership, business entity, sovereign, country or nation, will be limited to the greater of:

- \$100,000, or
- an amount equal to ten times the sum actually paid for the service alleged to be deficient.

The limitation of liability may be increased up to an amount 25 times that sum paid for services upon receipt of the Company's written request at or before the time of performance of services and upon payment by Company of an additional fee of \$10 for every \$1,000 increase in the limitation.

Also, for any services associated with this *Guide* provided to a Contracting Government, port operator, company, or other entity, the terms and conditions of the agreement between ABS Consulting and that entity will define all pertinent contractual requirements, including responsibilities of each part and associated liabilities.

## **1.5 DEFINITIONS**

*Company* is the owner, organization, or person responsible for the operation of a port facility.

*Declaration of Security (DOS)* is an agreement reached between a ship and port facility or another ship specifying the security measures each will implement.

*International Ship Security Certificate* is required by SOLAS and the International Ship and Port Facility Security Code.

*Organization* is the International Maritime Organization (IMO).

*Port* is the area through which ship traffic and maritime commerce flow or people are transported, including areas ashore (extending to intermodal and cargo storage areas) and on the adjacent water (to include anchorages and approaches), as defined by the designated authority.

*Port facility* is a location where the ship/port interface takes place, including anchorages, berths, and approaches.

*Port State* is the Government exercising control over ports and territorial waters. Note: The IMO generally uses the term Contracting Government to indicate the national government authority the maritime community thinks of as the Port State. The term “Contracting Government” reflects a level of involvement in IMO activities; however, it is expected that Port States that are not Contracting Governments in IMO terms will implement the requirements of the ISPS Code in order to allow their ports to participate in international trade.

*Recognized Security Organization* is an organization with appropriate expertise in security and antiterrorism matters recognized by a Contracting Government (for port/port facilities), or a Flag Administration (for vessels/ships), or their designated authorities, and authorized to carry out specific activities required by SOLAS Chapter XI-2 or by Part A of the ISPS Code on its behalf.

*Security incident* is any suspicious act or circumstance threatening the security of a ship, port, or port facility.

*Security level* is an action level established by an Administration or Contracting Government that represents its assessment of the likelihood that a security incident will be attempted or will occur.

*Ship* is any vessel, including a mobile offshore drilling unit, that is required to have an International Ship Security Certificate or other security certificate required by a government.

*Ship/Port interface* means the interactions that occur involving movement of people, goods, or provisions of port services to or from the ship.

*Ship-to-ship activity* is any activity not related to a port facility that involves the transfer of goods or persons from one ship to another.

*Statement of Compliance* is a document issued by a Contracting Government, or a Recognized Security Organization designated by a Contracting Government, that a port facility satisfies the requirements of its ‘approved’ Port Facility Security Plan based on an initial or interim verification of port security activities.

Note: The definition provided above for Statement of Compliance is drawn from the ISPS Code. If requested by a port facility, ABS Consulting will also verify compliance with the requirements of this *Guide* and issue a Statement of Compliance that indicates compliance with this *Guide*.

## **1.6 REFERENCES**

The references provided in this *Guide* include international standards and selected government and industry guidance documents. Excerpts from Chapter XI-2, “Special Measures to Enhance Maritime Security” of SOLAS 74 and excerpts from the text of the ISPS Code are reproduced verbatim for the reader’s use with the permission of the International Maritime Organization.

### **1.6.1 International Security Requirements**

- (i) SOLAS Chapter XI-2, “Special Measures to Enhance Maritime Security,” December 2002.
- (ii) ISPS Code Part A – *Mandatory Requirements Regarding the Provisions of Chapter XI-2 of the International Convention for the Safety of Life at Sea, 1974 as Amended*, December 2002.

### **1.6.2 International and Selected Government Guidance Documents**

- (i) ISPS Code Part B – *Guidance Regarding the Provisions of Chapter XI-2 of the Annex to the International Convention for the Safety of Life at Sea, 1974 as Amended*, December 2002.
- (ii) *Security Guidelines for Vessels*, NVIC Circular No. 10-02, USCG, October 2002.
- (iii) *Guidelines for Port Security Committees and Port Security Plans Required for U.S. Ports*, NVIC Circular No. 9-02, USCG, September 2002.
- (iv) *Security for Passenger Vessels and Passenger Terminals*, NVIC 4-02, USCG, April 2002.
- (v) *Recommended Security Guidelines for Facilities*, NVIC 11-02, USCG, January 2003.
- (vi) Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, and the Committee of the Regions on Enhancing Maritime Transport Security, *Proposal for a Regulation of the European Parliament and of the Council on Enhancing Ship and Port Facility Security*, May 2, 2003, COM(2003) 229 Final.

### **1.6.3 Other Useful References**

- (i) *ABS Guide for Ship Security*, American Bureau of Shipping, January 2003.
- (ii) *Piracy and Armed Robbery Against Ships*, Marine Notice 28/2002, Australian Maritime Safety Authority, Canberra City, AU ACT 2601, December 2002.
- (iii) *Piracy and Armed Robbery Toward Ships*, Port Marine Circular No. 23 of 2002, Maritime and Port Authority of Singapore, December 2002.
- (iv) *Piracy and Armed Robbery Against Ships – Guidance to Shipowners and Ship Operators, Shipmasters, and Crews on Preventing and Suppressing Acts of Piracy and Armed Robbery Against Ships*, MSC/Circ.623/Rev.3, International Maritime Organization, May 2002.
- (v) *Proposed Security Manual for Ships and Mobile Offshore Drilling Units*, Republic of Liberia, MSC 75/INF 27, April 2002.
- (vi) *AWO Model Vessel Security Plan*, The American Waterways Operators, Arlington, VA 22203, April 2002.
- (vii) *Marine Safety – Tools for Risk-based Decision Making*, ABS Consulting, Government Institutes, Rockville, MD 20850, 2002.
- (viii) *Guidance for Shipowners, Ship Operators, and Masters on the Protection of Ships from Terrorism and Sabotage*, International Chamber of Shipping, London, England, November 2001.
- (ix) *Safety and Security at Sea*, Butterworth-Heinemann, Woburn, MA 01801, 2000.
- (x) *Security at Sea – Terrorism, Piracy, and Drugs*, The Nautical Institute, London, England SE1 7LQ, 1991.



## 2. MARITIME SECURITY

### 2.1 GENERAL

Maritime security can only be achieved by cooperative efforts among all the parties involved in the maritime industries, with primary emphasis on ships, port facilities, and governments. Although this *Guide* applies only to port facilities that wish to obtain a Statement of Compliance from ABS Consulting, this section provides additional background information that might help in understanding the international security regime. This section (1) provides a general overview of the port facility security process and (2) describes security levels and the roles of governments in applying maritime security programs. Information on security requirements for ships is included to place the requirements for port facilities in perspective. It also provides an overview of the elements of basic security systems.

### 2.2 PROCESS OVERVIEW

The Company or Government Agency operating the port facility (i.e., the port operator) is responsible for setting the security policies for the port facility. As a minimum, those policies must conform to international and domestic requirements, but they should also reflect the port operator's objectives in maintaining safety and security on board its vessels, wherever they operate. The elements of a port facility security program should include the following:

- *Port Facility Security Officer (PFSO)* – An individual in the port operation's organization who is responsible for developing and implementing the port operator's security plan.
- *Port Facility Security Assessment* – A risk-based analysis of security-related threats to the port facility. The Port Facility Security Assessment should address (1) the particulars of the port facility, (2) the types of ships, cargoes, and passengers it serves, and (3) the locations from which cargo or passengers are accepted. It should also consider the likelihood of various security-related scenarios and possible responses to those scenarios.
- *Port Facility Security Plan* – A port facility-specific document based on the Port Facility Security Assessment that identifies equipment, measures, and procedures that are to be employed to maintain security at the port facility. The plan must address specific measures appropriate to the level of security specified by the Contracting Government.
- *Documentation* – Records and certificates that confirm that the port facility is in compliance with applicable security requirements. These may include records of security incidents, training, drills, and a Statement of Compliance with this *Guide*.

There are similar and corresponding security requirements in the ISPS Code requiring ships in international service to maintain appropriate levels of security. Those requirements include designating Ship Security Officers (SSOs) for each ship and Company Security Officers for each company operating ships covered by the ISPS Code. Those requirements are beyond the scope of this *Guide*. However, there are situations where the PFSO must communicate with SSOs (and in some cases, Company Security Officers) so that all parties understand the security condition of the ship and the port facility. The intent is that security is maintained while the ship is in port, and that all parties understand and are capable of taking what additional security measures are necessary if the security level changes while the ship is in port. The *ABS Guide for Ship Security*, which was developed to assist ship owners and operators to comply with the ISPS Code, can also serve as a valuable reference for a port operator and a PFSO.

### 2.3 **SECURITY LEVELS**

Chapter XI-2 of SOLAS requires that passenger ships, cargo ships over 500 gross tons, high-speed cargo and passenger ships, and mechanically propelled MODUs, on international voyages after July 1, 2004, are required to operate at a specified security level at all times. This requirement may be extended by governments to other ships flying their flags or entering their ports. The setting of the security level applicable at any particular time is normally the responsibility of a Flag Administration (for general application to ships flying their flags) and of a Contracting Government for port facilities under their control and ships visiting those facilities. In general, Ship and Port Facility Security Plans must address the measures to be taken at each security level. The three security levels used in international regulations and in this *Guide* are:

- *Security Level 1 (normal)*: the level at which ships and port facilities normally operate
- *Security Level 2 (heightened)*: the level applying for as long as there is a heightened risk of a security incident
- *Security Level 3 (exceptional)*: the level applying for the period of time when there is a probable or imminent risk of a security incident

### 2.4 **ADMINISTRATIONS**

Flag Administrations have a variety of security responsibilities for ships registered under their authority. These include:

- Providing guidance on the development of Ship Security Plans
- Providing guidance on measures for ships to implement at each security level
- Providing guidance on the reporting of attacks on ships
- Approving Ship Security Plans
- Issuing International Ship Security Certificates (ISSCs) to ships
- Notifying ships of appropriate security levels
- Notifying other governments of ship security alerts from ships within their jurisdiction
- Specifying requirements for Declarations of Security
- Agreeing to temporary measures to be implemented if security equipment fails
- Deciding whether or not to delegate approval of Ship Security Plans, verification of ship security systems, and issuance of ISSCs to Recognized Security Organizations and overseeing such delegations

### 2.5 **CONTRACTING GOVERNMENTS**

Governments that have jurisdiction over port facilities are responsible for:

- Designating the port facilities in their jurisdiction, which must have a Port Facility Security Officer and a Port Facility Security Plan
- Ensuring completion of a Port Facility Security Assessment for those port facilities
- Reviewing Port Facility Security Assessments and Port Facility Security Plans to ensure they meet the requirements of the ISPS Code
- Approving the Port Facility Security Plans and relevant amendments to approved plans
- Establishing points of contact within the government for reporting security concerns

- Setting the security levels
- Notifying affected parties of changes in security levels
- Defining when a Declaration of Security must be completed between a ship and a port facility

Where ABS Consulting has received authorization from a Contracting Government to act as a Recognized Security Organization for port facility security, and the Contracting Government has specified requirements that exceed those in this *Guide*, those requirements will become part of the items to be reviewed by ABS Consulting in the compliance verification performed on behalf of that Contracting Government.



### **3. CONTRACTING GOVERNMENT RESPONSIBILITIES**

The “International Requirements” listed in this section are extracted from the SOLAS language and the ISPS Code; however, in some cases, they have been paraphrased or reorganized for clarity. If there is any question regarding specific international requirements, the reader should refer to the language of the original documents. The latest versions are available directly from IMO at [www.imo.org](http://www.imo.org).

#### **3.1 PORT SECURITY ASSESSMENTS**

You will note that this section is titled “Port Security Assessments.” We have chosen to use the term as implemented by the USCG. It implies the higher-level assessment the ISPS Code requires the Contracting Government to prepare. We recognize that the ISPS Code language (as used in Section 3.1.1) is “port facility security assessment”; however, we believe that term (Port Facility Security Assessment) makes more sense for the plans that are typically being developed by owners and operators of individual terminals and other locations where interfaces occur with international ships covered by the ISPS Code. Such lower-level security assessments are required for each port facility only if a Contracting Government mandates them in addition to the Port Facility Security Plan required by the ISPS Code (see Section 4.4 of this Guide).

##### **3.1.1 International Requirements**

- a. SOLAS Chapter XI-2  
No specific requirements.
- b. ISPS Code Part A  
**Section 15 Port Facility Security Assessment**
  1. The Port Facility Security Assessment is an essential and integral part of the process of developing and updating the Port Facility Security Plan.
  2. The Port Facility Security Assessment shall be carried out by the Contracting Government within whose territory the port facility is located. A Contracting Government may authorize a Recognized Security Organization to carry out the Port Facility Security Assessment of a specific port facility located within its territory.
    - 2.1 When the Port Facility Security Assessment has been carried out by a Recognized Security Organization, the security assessment shall be reviewed and approved for compliance with this section by the Contracting Government within whose territory the port facility is located.
  3. The persons carrying out the assessment shall have appropriate skills to evaluate the security of the port facility in accordance with this section, taking into account the guidance given in Part B of this Code.
  4. The Port Facility Security Assessments shall periodically be reviewed and updated, taking account of changing threats and/or minor changes in the port facility and shall always be reviewed and updated when major changes to the port facility take place.

5. The Port Facility Security Assessment shall include, at least, the following elements:
  - identification and evaluation of important assets and infrastructure it is important to protect;
  - identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures;
  - identification, selection, and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability; and
  - identification of weaknesses, including human factors in the infrastructure, policies, and procedures.
6. The Contracting Government may allow a Port Facility Security Assessment to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar. Any Contracting Government, which allows such an arrangement, shall communicate to the Organization particulars thereof.
7. Upon completion of the Port Facility Security Assessment, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment, and a description of countermeasures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

### **3.1.2 ABS Consulting Guidance**

One of the decisions a Contracting Government needs to make is how it is going to perform Port and Port Facility Security Assessments required by the ISPS Code. There are a couple of questions that need to be answered:

- Are Contracting Government personnel going to perform the security assessment themselves?
- Is the Contracting Government going to designate Recognized Security Organizations to perform the security assessment?
- Are port authorities going to be appointed as Recognized Security Organizations to perform their own security assessments?

Contracting Governments are expected to make these decisions based on their internal capability to perform assessments, the resources available to them, and how sophisticated their port authorities are. ABS Consulting suggests that security assessments should be performed by organizations that have the ability to base the assessments on examination of specific threat scenarios, with consideration of the vulnerability of the port and ships in the port and the consequence of those scenarios. The USCG interim maritime security regulations indicate that NVIC 9-02 and NVIC 11-02 are acceptable approaches for Port and Port Facility Security Assessments, respectively. However, other Contracting Governments are in the process of defining their own guidance for the performance of Port and Port Facility Security Assessments. ABS Consulting will work with government authorities, port operators, and port facility operators to help them define security assessment approaches that will satisfy the ISPS Code requirements and address local needs. Appendix 1 to this

document provides guidance on how Port and Port Facility Security Assessments can be performed.

### **3.2 VERIFICATION OF COMPLIANCE FOR PORT FACILITIES**

#### **3.2.1 International Requirements**

- a. SOLAS Chapter XI-2  
No specific requirements.
- b. ISPS Code Part A  
No specific requirements.

#### **3.2.2 ABS Consulting Guidance**

If ABS Consulting is authorized by a Contracting Government to review implementation of a Port Facility Security Plan that has been approved by the Contracting Government, the following recommendations from Part B of the ISPS Code (Sections 16.62 and 16.63) will be implemented:

- a. ABS Consulting will issue a Statement of Compliance for the port facility, indicating:
  1. the port facility;
  2. that the port facility complies with the provisions of Chapter XI-2 and Part A of the ISPS Code as defined in the approved Port Facility Security Plan;
  3. the period of validity of the Statement of Compliance (which should be specified by the Contracting Governments but should not exceed 5 years); and
  4. the subsequent verification arrangements established by the Contracting Government and a confirmation when these are carried out.
- b. The Statement of Compliance will be in the form set out in Appendix 1 to Part B of the ISPS Code, with any changes specified by the Contracting Government responsible for the port facility involved.

### **3.3 ALTERNATIVE AGREEMENTS AND EQUIVALENT REQUIREMENTS**

#### **3.3.1 International Requirements**

- a. SOLAS Chapter XI-2

#### **Regulation 11 Alternative Security Agreements**

1. Contracting Governments may, when implementing this chapter and Part A of the ISPS Code, conclude in writing bilateral or multilateral agreements with other Contracting Governments on alternative security arrangements covering short international voyages on fixed routes between port facilities located within their territories.
2. Any such agreement shall not compromise the level of security of other ships or of port facilities not covered by the agreement.

3. No ship covered by such an agreement shall conduct any ship-to-ship activities with any ship not covered by the agreement.
4. Such agreements shall be reviewed periodically, taking into account the experience gained as well as any changes in the particular circumstances or the assessed threats to the security of the ships, the port facilities, or the routes covered by the agreement.

#### **Regulation 12 Equivalent Security Arrangements**

1. An Administration may allow a particular ship or a group of ships entitled to fly its flag to implement other security measures equivalent to those prescribed in this chapter or in Part A of the ISPS Code, provided such security measures are at least as effective as those prescribed in this chapter or Part A of the ISPS Code. The Administration, which allows such security measures, shall communicate to the Organization particulars thereof.
  2. When implementing this Chapter and Part A of the ISPS Code, a Contracting Government may allow a particular port facility or a group of port facilities located within its territory, other than those covered by an agreement concluded under Regulation 11, to implement security measures equivalent to those prescribed in this chapter or in Part A of the ISPS Code, provided such security measures are at least as effective as those prescribed in this chapter or Part A of the ISPS Code. The Contracting Government, which allows such security measures, shall communicate to the Organization particulars thereof.
- b. ISPS Code Part A  
No specific requirements.

#### **3.3.2 ABS Consulting Guidance**

No additional guidance provided.

## **4. PORT FACILITY RESPONSIBILITIES**

The “International Requirements” listed in this section are extracted from the SOLAS language and the ISPS Code. However, in some cases, they have been paraphrased or reorganized for clarity. If there is any question regarding specific international requirements, the reader should refer to the language of the original documents.

### **4.1 PORT FACILITY**

#### **4.1.1 International Requirements**

a. SOLAS Chapter XI-2

**Regulation 10 Requirements for Port Facilities**

1. Port facilities shall comply with the relevant requirements of this chapter and Part A of the ISPS Code, taking into account the guidance given in Part B of the ISPS Code.
2. Contracting Governments with a port facility or port facilities within their territory, to which this regulation applies, shall ensure that:
  - Port Facility Security Assessments are carried out, reviewed, and approved in accordance with the provisions of Part A of the ISPS Code; and
  - Port Facility Security Plans are developed, reviewed, approved, and implemented in accordance with the provisions of Part A of the ISPS Code.
3. Contracting Governments shall designate and communicate the measures required to be addressed in a Port Facility Security Plan for the various security levels, including when the submission of a Declaration of Security will be required.

b. ISPS Code Part A

**Section 14 Port Facility Security**

1. A port facility is required to act upon the security levels set by the Contracting Government within whose territory it is located. Security measures and procedures shall be applied at the port facility in such a manner as to cause a minimum of interference with, or delay to, passengers, ship, ship’s personnel and visitors, goods and services.
2. At Security Level 1, the following activities shall be carried out through appropriate measures in all port facilities, taking into account the guidance given in Part B of this Code, in order to identify and take preventive measures against security incidents:
  - ensuring the performance of all port facility security duties;
  - controlling access to the port facility;
  - monitoring of the port facility, including anchoring and berthing area(s);

- monitoring restricted areas to ensure that only authorized persons have access;
  - supervising the handling of cargo;
  - supervising the handling of ship's stores; and
  - ensuring that security communication is readily available.
3. At Security Level 2, the additional protective measures, specified in the Port Facility Security Plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in Part B of this Code.
  4. At Security Level 3, further specific protective measures, specified in the Port Facility Security Plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in Part B of this Code.
    - In addition, at Security Level 3, port facilities are required to respond to and implement any security instructions given by the Contracting Government within whose territory the port facility is located.
  5. When a Port Facility Security Officer is advised that a ship encounters difficulties in complying with the requirements of chapter XI-2, or this part, or in implementing the appropriate measures and procedures as detailed in the Ship Security Plan, and in the case of Security Level 3, following any security instructions given by the Contracting Government within whose territory the port facility is located, the Port Facility Security Officer and Ship Security Officer shall liaise and coordinate appropriate actions.
  6. When a Port Facility Security Officer is advised that a ship is at a security level, which is higher than that of the port facility, the Port Facility Security Officer shall report the matter to the competent authority and shall liaise with the Ship Security Officer and coordinate appropriate actions, if necessary.

#### **4.1.2 ABS Consulting Guidance**

No additional guidance provided.

## **4.2 PORT FACILITY SECURITY OFFICER**

### **4.2.1 International Requirements**

- a. SOLAS Chapter XI-2  
No specific requirements.

- b. ISPS Code Part A

#### **Section 2 – Definitions**

*Port Facility Security Officer* means the person designated as responsible for the development, implementation, revision, and maintenance of the Port Facility Security Plan and for liaison with the Ship Security Officers and Company Security Officers.

## **Section 17 Port Facility Security Officer**

1. A Port Facility Security Officer shall be designated for each port facility. A person may be designated as the Port Facility Security Officer for one or more port facilities.
2. In addition to those specified elsewhere in this part of the Code, the duties and responsibilities of the Port Facility Security Officer shall include, but are not limited to:
  - conducting an initial comprehensive security survey of the port facility taking into account the relevant Port Facility Security Assessment;
  - ensuring the development and maintenance of the Port Facility Security Plan;
  - implementing and exercising the Port Facility Security Plan;
  - undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;
  - recommending and incorporating, as appropriate, modifications to the Port Facility Security Plan in order to correct deficiencies and to update the plan to take into account of relevant changes to the port facility;
  - enhancing security awareness and vigilance of the port facility personnel;
  - ensuring adequate training has been provided to personnel responsible for the security of the port facility;
  - reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;
  - coordinating implementation of the Port Facility Security Plan with the appropriate Company and Ship Security Officer(s);
  - coordinating with security services, as appropriate;
  - ensuring that standards for personnel responsible for security of the port facility are met;
  - ensuring that security equipment is properly operated, tested, calibrated, and maintained, if any; and
  - assisting Ship Security Officers in confirming the identity of those seeking to board the ship when requested.
3. The Port Facility Security Officer shall be given the necessary support to fulfill the duties and responsibilities imposed by chapter XI-2 and this part of this Code.

### **4.2.2 ABS Consulting Guidance**

No additional guidance provided.

### 4.3 **PORT FACILITY SECURITY ASSESSMENTS**

There is no ISPS Code requirement for each port facility operator to perform a facility security assessment. The assessment that the ISPS Code requires, and which is called a “port facility security assessment,” has to be performed by the Contracting Government and is addressed in Section 3.1 of this *Guide*. This section is provided to remind facility operators that they need to determine if their Contracting Government has required each port facility to perform some level of specific facility assessment. For example, the USCG maritime security regulation for facilities requires every facility to perform a facility security assessment (see 33 CFR 105 Subpart C). The USCG defines an acceptable methodology for such an assessment in NVIC 11-02, “Security Guidelines for Facilities.”

### 4.4 **PORT FACILITY SECURITY PLANS**

#### 4.4.1 **International Requirements**

a. SOLAS Chapter XI-2  
No specific requirements.

b. ISPS Code Part A

#### **Section 16 Port Facility Security Plan**

1. A Port Facility Security Plan shall be developed and maintained, on the basis of a Port Facility Security Assessment, for each port facility, adequate for the ship/port interface. The plan shall make provisions for the three security levels, as defined in this part of the Code.

1.1 Subject to the provisions of section 16.2, a Recognized Security Organization may prepare the Port Facility Security Plan of a specific port facility.

2. The Port Facility Security Plan shall be approved by the Contracting Government in whose territory the port facility is located.

3. Such a plan shall be developed taking into account the guidance given in Part B of this Code and shall be in the working language of the port facility. The Plan shall address, at least, the following:

- measures designed to prevent weapons or any other dangerous substances and devices intended for use against people, ships or ports and the carriage of which is not authorized, from being introduced into the port facility or onboard a ship;
- measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restricted areas of the facility;
- procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface;
- procedures for responding to any security instructions the Contracting Government, in whose territory the port facility is located, may give at Security Level 3;

- procedures for evacuation in case of security threats or breaches of security;
- duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects;
- procedures for interfacing with ship security activities;
- procedures for the periodic review of the plan and updating;
- procedures for reporting security incidents;
- identification of the Port Facility Security Officer, including 24-hour contact details;
- measures to ensure the security of the information contained in the plan;
- measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility;
- procedures for auditing the Port Facility Security Plan;
- procedures for responding in case the ship security alert system of a ship at the port facility has been activated; and
- procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers' welfare and labor organizations.

3.1 Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the port facility.

4. The Port Facility Security Plan may be combined with, or be part of, the port security plan or any other port emergency plan or plans.
5. The Contracting Government in whose territory the port facility is located shall determine which changes to the Port Facility Security Plan shall not be implemented unless the relevant amendments to the plan are approved by them.
6. The Plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.
7. The Plan shall be protected from unauthorized access or disclosure.
8. Contracting Governments may allow a Port Facility Security Plan to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar. Any Contracting Government, which allows such an alternative arrangement, shall communicate to the Organization particulars thereof.

## 4.4.2 *ABS Consulting Guidance*

### 4.4.2.1 Delegation of Authority

The Port Facility Security Plan should state that the PFSO has the authority to report directly to the highest level of port facility operations management for matters of security.

### 4.4.2.2 Maritime Domain Security Awareness Program

The Port Facility Security Plan should also include a requirement for the PFSO to maintain awareness of security threat information (e.g., intelligence reports, reports of suspicious activities, criminal activity) for the areas in which the port facility is located. That information should be used in performing Port Facility Security Assessments and should be reviewed periodically to assist in security planning and implementation.

The first source of maritime domain awareness information should be reports by the stakeholders in the port facility and other nearby facilities. This information should be solicited from employees, contractors, ship crews, visitors, and neighboring facilities. In addition, liaisons with appropriate law enforcement agencies should be maintained in order to take advantage of any security threat information available from those organizations.

In addition to contacting local and law enforcement sources for maritime security threat information, some publicly available sources for such information exist, including:

- The U.S. Office of Naval Intelligence's weekly *World Wide Threat to Shipping* report. It is available at: [http://164.214.12.145/onit/onit\\_j\\_main.html](http://164.214.12.145/onit/onit_j_main.html)
- The International Maritime Bureau's Weekly *Piracy Report* is available at: [http://www.iccwbo.org/ccs/imb\\_piracy/weekly\\_piracy\\_report.asp](http://www.iccwbo.org/ccs/imb_piracy/weekly_piracy_report.asp)

Both of these sources provide reports of attacks on shipping, whether from terrorist activity or piracy; however, they are also useful to help port facility personnel understand the threats faced by ships using their port. This information can help provide a picture of what types of security measures need to be implemented.

### 4.4.2.3 Coordinated Security Plans

It is expected that most Contracting Governments will implement some form of "coordinated" security plans (the USCG plan is called a "family of plans"). For example, the Contracting Government generally has some form of maritime authority that exercises port state control functions, one of which is ensuring that ships entering the country's ports have approved security plans. It is expected that Contracting Governments will also provide guidance to its port facilities regarding what security measures individual port facilities must maintain to supplement whatever measures the Contracting Government or its port authority provides on a portwide basis. This can most easily be done by developing a "Port Security Plan" that then requires individual "Port Facility Security Plans" for designated port facilities. Please recognize that the ISPS Code does not address the issue of plans at different levels. It only refers to "port facility," which is defined as the location where the ship/port interface occurs.

#### 4.4.2.4 Example Port Facility Security Plan

An example Port Facility Security Plan (PFSP) is included in Appendix 2 to this *Guide*. The example illustrates one port facility's approach for documenting what is required by the ISPS Code. Parts A and B of the ISPS Code provide the requirements and guidance, respectively, for the contents of a PFSP.

The example in Appendix 2 is included as an example (only) of the categories and types of information that a PFSP should address and document. Compared to different classes of marine vessels, ports and port facilities are subject to a much greater degree of variability in a broader range of characteristics. Thus, it is important that users of this *Guide* do not consider the example PFSP to be a standard by which other PFSPs should be developed and measured.

PFSPs are subject to many variables, including but not limited to:

- General requirements of Contracting Governments or their designated authorities, including security provisions that may be specified for each security level
- Specific requirements of an upper-level Port Security Plan, specified by a Contracting Government or its designated authority, with which facilities in the port must comply
- Port geography, topography, natural and artificial barriers and their configurations, and the proximity of specific port facilities to each other and to the infrastructure of the port in which such port facilities are located
- Specific characteristics (security risks/exposures) of other port facilities located in the same port (e.g., types of ships, cargoes, goods, passengers, and/or services handled by other facilities in the same port)
- Specific operating, management, and security characteristics/risks of the particular port facility for which PFSP is established

These variations mean that no single PFSP can illustrate all the potential security measures and procedures that may be required for other port facilities to meet the requirements and guidance of the ISPS Code.

## 4.5 TRAINING AND DRILLS

### 4.5.1 International Requirements

- a. SOLAS Chapter XI-2  
No specific requirements.
- b. ISPS Code Part A,  
**Section 18 Training and Drills**
  1. The Port Facility Security Officer and appropriate port facility security personnel shall have knowledge and have received training, taking into account the guidance given in Part B of this Code.
  2. Port facility personnel having specific security duties shall understand their duties and responsibilities for port facility security, as described in the Port Facility Security Plan and shall have sufficient knowledge and ability to

perform their assigned duties, taking into account the guidance given in Part B of this Code.

3. To ensure the effective implementation of the Port Facility Security Plan, drills shall be carried out at appropriate intervals taking into account the types of operations of the port facility, port facility personnel changes, the type of ship the port facility is serving and other relevant circumstances, taking into account guidance given in Part B of this Code.
4. The Port Facility Security Officer shall ensure the effective coordination and implementation of the Port Facility Security Plan by participating in exercises at appropriate intervals, taking into account the guidance given in Part B of this Code.

#### **4.5.2 ABS Consulting Guidance**

In addition to specific training for personnel who are involved in implementing security actions, all port facility employees should receive security awareness training as part of their general orientation and training activities. This awareness training should address issues such as:

- Limiting discussion about specifics of the port facility (e.g., security plans; security personnel; and equipment, cargoes, and schedules) to those personnel who need to know in order to provide support to port and ship activities
- Reporting suspicious acts or behavior at or near the port when recognized
- Protection of port facility identification cards or other documentation

A high level of awareness by port facility personnel and knowledge of these simple measures can help prevent port assets and ships in the port from becoming easy targets of security threats.

### **4.6 SECURITY RECORDS**

#### **4.6.1 International Requirements**

- a. SOLAS Chapter XI-2  
No specific requirements.
- b. ISPS Code Part A  
No specific requirements.

#### **4.6.2 ABS Consulting Guidance**

The Port Facility Security Plan should make provision for the retention of records of security incidents and threats, reviews, audits, training, and drills and exercises as evidence of compliance with requirements related to those activities (Part B, Section 16.5). Security-related records required under the international or national requirements, and any additional records specified by ABS Consulting, shall be kept for at least 2 years and longer if necessary to provide evidence of program compliance during any periodic verification required by the Contracting Government.

## **4.7 AUDITS AND REVIEWS**

### **4.7.1 International Requirements**

- a. SOLAS Chapter XI-2  
No specific requirements.
- b. ISPS Code Part A, Section 16 – Port Facility Security Plan  
The Port Facility Security Plan must include procedures for auditing the plan (Section 16.3.13). Also, personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless such independence is impracticable due to the size and the nature of the port facility (Section 16.3.1).

### **4.7.2 ABS Consulting Guidance**

The security audit program description in the Port Facility Security Plan should define responsibility for resolving audit findings and reporting the status of open security audit findings to port facility management. Internal audits of the Port Facility Security Plan and its effective implementation should be carried each calendar year, not to exceed 18 months between audits. A periodic report of the status of audit findings should be available at the port facility. Records of the corrective actions addressing those findings must be documented as well. A copy of this internal audit report, a current status report for the audit findings, and documentation of the corrective actions for closed findings should be maintained at the port facility for verification purposes.

## **4.8 DECLARATION OF SECURITY**

### **4.8.1 International Requirements**

- a. SOLAS Chapter XI-2  
**Regulation 1 Definitions**  
*Declaration of Security* means an agreement reached between a ship and either a port facility or another ship with which it interfaces specifying the security measures each will implement.
- b. ISPS Code Part A, Section 5 – Declaration of Security
  1. Contracting Governments shall determine when a Declaration of Security is required by assessing the risk the ship/port interface or ship-to-ship activity poses to people, property or the environment.
  2. A ship can request completion of a Declaration of Security when:
    - the ship is operating at a higher security level than the port facility or another ship it is interfacing with;
    - there is an agreement on Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages;
    - there has been a security threat or a security incident involving the ship or involving the port facility, as applicable;

- the ship is in a port which is not required to have and implement an approved Port Facility Security Plan; or
  - the ship is conducting ship-to-ship activities with another ship not required to have and implement an approved Ship Security Plan.
3. Requests for the completion of a Declaration of Security, under this section, shall be acknowledged by the applicable port facility or ship.
  4. The Declaration of Security shall be completed by:
    - the Master or the Ship Security Officer on behalf of the ship(s); and, if appropriate,
    - the Port Facility Security Officer or, if the Contracting Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility
  5. The Declaration of Security shall address the security requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibility for each.
  6. Contracting Governments shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by the port facilities located within their territory.
  7. Administrations shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by ships entitled to fly their flag.

#### **4.8.2 ABS Consulting Guidance**

No additional guidance provided.

***APPENDIX 1***

***Guidance for Performing Port and Port Facility  
Security Assessments***

### ***A.1.1 INTRODUCTION***

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. A security assessment may also suggest options to eliminate or mitigate those weaknesses. Section A.1.2 of this appendix describes the ISPS Code requirements for performing security assessments to help in developing security plans. Section A.1.3 describes how the USCG is developing security assessments to address ISPS Code requirements and discusses the issues that Contracting Governments need to consider in defining their own approach for conducting the security assessments required under the ISPS Code. Section A.1.4 describes the risk management basis for security assessments, and Section A.1.5 provides guidance on how port security assessments can be performed and documented.

### ***A.1.2 ISPS CODE PORT FACILITY REQUIREMENTS***

Regulation 1 of Chapter XI-2 of SOLAS provides some of the definitions that apply to the ISPS Code, including ones for ship/port interface and port facility:

*“Ship/port interface means the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services to or from the ship.”*

*“Port facility is a location, as determined by the Contracting Government or by the Designated Authority, where the ship/port interface takes place. This includes areas such as anchorages, waiting berths and approaches from seaward, as appropriate.”*

These definitions encompass areas in which security is generally the responsibility of government authorities (e.g., approaches and anchorages) and areas where security is largely the responsibility of government or commercial organizations operating waterfront facilities (e.g., docks and terminals). However, the ISPS Code only defines a requirement for “port facility security assessments” that are the responsibility of the Contracting Government.

Contracting Governments are required to conduct Port Facility Security Assessments (PFSAs) themselves or to authorize a Recognized Security Organization (RSO) to perform PFSAs for the government (Part A, Section 15.2). If the PFSA is not performed by the Government, the Government is required to review and approve the assessment (Part A, Section 15.2.1). Regardless of who performs the PFSA, the ISPS Code requires that the team members for the assessment either have specific skills or be able to draw on other resources that can provide those skills (Part A, Section 15.3 and Part B, Section 15.4).

The IMO ISPS Code (Part A, Section 15.5) requires that the PFSA include at least the following elements:

- identification and evaluation of assets and infrastructure it is important to protect;
- identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures;

- identification, selection, and prioritization of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability; and
- identification of weaknesses, including human factors in the infrastructure, policies, and procedures.

All of the additional guidance regarding PFSAs is provided in Part B of the ISPS Code, Sections 15.5 through 15.16.

Upon completion of the PFSA, a report must be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment, and a description of countermeasures that could be used to address each vulnerability. The report must be protected from unauthorized access or disclosure (Part A, Section 15.7).

The PFSA must be periodically reviewed and updated, taking into account changing threats and/or minor changes in the port facility and must be reviewed and updated when major changes to the port facility take place (Part A, Section 15.4).

### ***A.1.3 NATIONAL APPROACHES TO MEETING ISPS PORT SECURITY ASSESSMENT REQUIREMENTS***

#### **United States Approach**

Because there are generally government and commercial entities that will need to develop security plans, both types of organizations need to be involved in the security assessment activities that are needed to support the development of effective security plans. In the United States, the U.S. Coast Guard (USCG) has developed an approach that will develop two types of security assessments. The USCG Captain of the Port for each of the U.S. ports is responsible for putting together a Port Security Committee that will provide the stakeholder input to allow the USCG to perform a Port Security Assessment. The approach for that assessment is defined in the USCG guidance document for port security, *Guidelines for Port Security Committees and Port Security Plans Required for U.S. Ports*, NVIC Circular No. 9-02, USCG, September 2002. That Security Assessment and the Port Security Plan, to be developed based in part on the assessment results, are the documents that will be reported to the IMO as satisfying the ISPS Code requirements. However, the USCG is also requiring individual facilities, which serve international ships that are subject to the ISPS Code requirements, to perform their own “facility security assessment.” (In addition, the USCG has expanded the scope of U.S. regulations to require Ship and Port Facility Security Assessments for many vessels and facilities that do not fall under the ISPS Code requirements.) The USCG guidance for performing facility security assessments is provided in *Recommended Security Guidelines for Facilities*, NVIC 11-02, USCG, January 2003.

#### **Other Contracting Government Approaches**

Other Contracting Governments are also defining their approaches for meeting the ISPS Code requirements for “port facility security assessments.” It is expected that some countries will use a two-level assessment approach like the USCG approach described above. However, there are many different ways that the ISPS Code requirements can be met. ABS Consulting suggests that the approach used by each country be developed based on national priorities, government agency

staffing and expertise, available funding, and existing regulatory approaches. We do not believe that the USCG approach is the right way to proceed for all countries. ABS Consulting has provided training and services to support several countries involved in deciding on an appropriate approach for ISPS Code compliance. We expect to continue to provide such services; however, the remainder of this appendix outlines the port security assessment approach adopted by the USCG (i.e., the upper tier of the two levels of Port and Port Facility Assessments being performed in the United States).

#### **A.1.4 BASIC RISK CONCEPTS FOR SECURITY ASSESSMENT PURPOSES**

Risk is generally expressed as the product of frequency (e.g., events per year) times consequence (e.g., fatalities per event, dollars per event, barrels of oil spilled per event). For the potential for relatively rare events to occur in a specific time frame, frequency is usually replaced by the probability of an event in that time frame. Therefore, for an individual scenario that poses undesirable consequences, risk can be represented by:

$$R = P * C \tag{Equation 1}$$

Where  
R = risk  
P = probability  
C = consequence

Consequence is the sum of possible effects of the attack given the scenario. These consequences may include all or some of several different categories of effects (e.g., death/injury, economic impacts, environmental effects), therefore the overall consequence is the sum of those effects, which can be shown as :

$$SC = C_{death/injury} + C_{economic} + C_{environment} + \dots \tag{Equation 2}$$

The continuation of that equation indicates that for any given risk assessment there may be other categories of consequence (e.g., impact on national defense, symbolic effects) that are of interest to the organization performing the risk assessment. Also, being able to add consequences implies that the organization can express all of the consequences in the same units (e.g., monetary units) or can define working equivalents (e.g., equivalent “pain levels”) for each type of consequence.

#### Frequency

In risk assessments other than security applications, the probability in Equation 1 is typically estimated from historical data or is calculated based on the likelihood of combinations of external events, human errors, and system/equipment failures that must occur for the consequences to be realized. However, for security purposes, the likelihood of a scenario is generally assessed by examining the specific threat to the security of a port or port facility and the vulnerability of the port or port facility to that threat. This can be shown as:

$$P = T * V \tag{Equation 3}$$

Where  
T = threat  
V = vulnerability

Threat represents the probability of an attack based on the existence of intelligence and maritime domain awareness. For maritime security, threat is reflected in the assignment of the security level and the approach that security measures are planned differently for various security levels. In a detailed security assessment, an estimate of the threat can be made and used to better assess the probability of an attack. However, for the security assessment approach described here, the threat level is assumed as a constant, so the risk is assessed based on the differences in vulnerability and consequence for each scenario examined. If a port or port facility operator has information that allows them to judge the relative threat to specific port facilities (or vessels within a port), that information can also be used by the security assessment team as another aspect to rank the relative risk of the port facilities and resources (e.g., infrastructure items)

Vulnerability is the probability of success of an attack and is assessed by examining factors that contribute to the vulnerability of the port or port facility. Four elements commonly used to assess vulnerability of assets are: availability, accessibility, organic security, and target hardness. These are not the only vulnerability criteria that could be used, but they address important issues in assessing maritime security risks.

#### ***A.1.5 SUGGESTED PORT SECURITY ASSESSMENT APPROACH***

The approach described here is based primarily on the USCG approach defined in NVIC 9-02 for port security assessments intended to satisfy the ISPS Code “port facility” security assessment requirement. It consists of:

- Criticality assessment
- Threat assessment
- Consequence assessment
- Vulnerability analysis

A **criticality assessment** (as suggested in NVIC 9-02) is a process designed to systematically identify and evaluate important assets and infrastructure in terms of various factors, such as the mission and significance of a target. For example, nuclear power plants, key bridges, and major computer networks might be identified as “critical” in terms of their importance to public safety, national security, and economic activity. In addition, facilities might be critical at certain times, but not others. For example, large sports stadiums, shopping malls, or office towers may represent an important target only when in use by large numbers of people. Criticality assessments are important because they provide a basis for focusing the mitigation strategies and implementation methods on the most important items by identifying which assets and structures are more crucial to protect from an attack. Criticality assessments consider such factors as the importance of a structure to the missions of the port, the ability to reconstitute this capability, and the potential cost to repair or replace the asset. Criticality assessments should also give information on impacts to life, economic security, symbolic value, and national defense. Criticality assessments provide information to prioritize assets and determine which potential targets merit further evaluation.

A **threat assessment** is used to evaluate the likelihood of attack against a given asset or location. It is a decision support tool that helps to establish and prioritize security-program requirements, planning, and resource allocations. A threat assessment identifies and evaluates each threat on the basis of various factors, including capability and intention. By identifying and assessing threats, organizations do not have to rely on worst-case scenarios to guide planning and resource allocations. Worst-case

scenarios tend to focus on extreme consequences and typically require inordinate resources to address.

While threat assessments are a key decision support tool, it should be recognized that they are dependent on intelligence data. Even if updated often, threat assessments might not adequately capture emerging threats. No matter how much we know about potential threats, we will never know that we have identified every threat or that we have complete information even about the threats of which we are aware. Threat assessments alone are insufficient to support key judgments and decisions that must be made.

The ISPS Code and USCG guidance documents do not provide an approach for threat assessment. However, the USCG guidance defines approaches for consequence assessment and vulnerability assessment. Even when a detailed threat assessment is not available, the consequence and vulnerability assessments provide a measure of how attractive a target is, which is a measure of threat.

A **consequence assessment** evaluates the negative impact of a successful attack. It is a method to evaluate the likely outcomes of a scenario. The consequence analysis promotes the consideration of an attack's impacts, including:

- Deaths and injuries
- Economic impacts
- Public safety/national defense effects
- Environmental impacts
- Symbolic effect

This assessment evaluates the consequence term of the risk equation.

A **vulnerability assessment** is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may lead to a security breach, and may suggest options to eliminate or mitigate those weaknesses. For example, a vulnerability assessment might reveal weaknesses in an organization's security systems or unprotected key infrastructure, such as water supplies, bridges, and tunnels. In general, teams of subject matter experts should conduct vulnerability assessments. For example, at many passenger terminals, experts have identified security concerns, including the distance from parking lots to important staging areas and buildings as being so close that a car bomb detonation would damage or destroy the buildings and kill people in them. To mitigate this threat, experts have advised to increase the distance between parking lots and buildings. Another security enhancement might be to reinforce the windows in buildings to prevent glass from flying into the building if an explosion occurs. Such assessments can identify vulnerabilities in port operations, personnel security, and physical and technical security.

After criticality, threat, consequence, and vulnerability assessments have been completed and evaluated in this risk-based decision process, key actions can be taken to better prepare against potential terrorist attacks.

Following is an approach for risk-based port security assessment that can be further refined and tailored to specific ports or port facilities. The overall steps of port security assessment are:

1. Perform a criticality assessment to identify critical activities or operations. This helps identify critical targets with the port, allowing them to be the focus of further assessments. For small ports or individual port facilities, a criticality assessment is not likely to be needed. For example, the USCG guidance for port security assessments (i.e., NVIC 9-02) includes an approach for criticality assessment, but the similar guidance for facility security assessments (i.e., NVIC 11-02) has no such approach.
2. Conduct a threat assessment to define scenarios by combining threats with credible attack scenarios.
3. Conduct consequence and vulnerability assessments for each target/scenario combination using a high, medium, low score based on descriptors of specific elements in Tables 3, 4, and 5. Table 3 lists several consequence criteria for use; Table 4 lists vulnerability categories to consider; and Table 5 lists vulnerability criteria. Note that consensus should be reached on a single overall consequence score and a single overall vulnerability score for each target/scenario combination.
4. Categorize the target/scenario combinations using Table 6. Table 6 prioritizes scenarios by organizing them into three categories: those for which mitigation strategies should be developed; those that should be considered on a case-by-case basis; and those that do not need mitigation strategies and need only to be documented.

Note: NVIC 9-02 includes an example approach for developing and evaluating proposed security measures that is not repeated here. It serves to help the Port Security Assessment (PSA) team ensure that effective security measures are adopted for specific vulnerabilities.

An expanded explanation of the steps follows.

## **STEP 1: CRITICALITY ASSESSMENT**

A Criticality Assessment helps identify activities and operations critical to a port. This will assist in target selection. Examples may include supporting a cruise line industry, ensuring throughput of needed feedstock materials for a petrochemical industry, or providing waterway access for commuter ferries.

Identify those specific infrastructure targets that support critical operations of the port. All identified targets should be included in the evaluation. Targets considered but dismissed for evaluation should be documented for future reference. While not all encompassing, Table 1 lists general classes of targets that should be considered. In addition, it is important to consider the role or mission of the target in the operation of the port. Broadly, we consider five mission or operation areas to be of interest. These are: public health, commerce, safety/defense, transportation, and communications. The effect of destruction considers which consequence factors are affected by the loss of the target. The next consideration in determining criticality is the ability to recover from destruction of the target. If an individual bridge is considered, but it is one of four parallel bridges crossing the same waterway, the ability of the port to recover from its destruction is likely to be better than if it is the only means. Finally, consider the number of mission areas affected, the degree of the effects, and the ability to recover and make an overall assessment of the criticality.

Criticality should be rated according to the following scale: Critical/Moderate/Marginal. Critical items support multiple mission areas, have several consequence effects, and are difficult or impossible to recover from in a timely manner. Moderate criticality targets may support one or two missions areas, affect one or two consequence areas, or have a reasonable ability to recover in a timely manner. Marginal criticality targets may not support any mission areas, may have limited to minimal effects of destruction, and may have backup or redundant systems in place that minimize recovery time.

Table 1 can be used to summarize the team’s rationale in identifying critical assets.

**Table 1 Criticality Assessment Format**

<b>Target</b>	<b>Mission</b>	<b>Effect of Target Destruction</b>	<b>Ability to Recover</b>	<b>Criticality</b>
Bridge	Public Health	Loss of Life	Excellent	Critical Moderate Marginal
Utility	Commerce	Economic Impact	Good	
Pier	Safety/Defense	Environmental Impact	Fair	
Tunnel	Transportation	Public Safety/Defense	Poor	
Waterway	Communications	Symbolic Significance	None	
Other	Other			

When feasible it is preferable to group identical targets at the specific target level. However, some targets may need to be considered individually. For example, a unique bridge should be considered individually given differences in communication cables, pipelines, and traffic that cross that bridge. The purpose of considering targets individually is to be specific enough to differentiate which targets need mitigation.

Large facilities, such as those operated by port authorities and consisting of many facilities, may sometimes be considered as one target or in other cases, subdivided into individual targets as appropriate based on the attack scenario. For example, an entire port may be the target in one attack scenario, but individual parts of it may be targets in other attack scenarios.

**STEP 2: THREAT ASSESSMENT AND SCENARIO SELECTION**

An attack scenario consists of a potential threat to a unique target or target class under specific circumstances. It is important that the developed scenario or scenarios are within the realm of possibility and, at a minimum, address known capabilities and intents as evidenced by past events and available intelligence. For example, a boat containing explosives (a specific class of scenario) ramming a tanker (target) that is outbound through a choke point (specific circumstance) is one credible scenario. It is much less credible that a U. S. Navy ship will be commandeered and used to ram a bridge unless specific intelligence reports indicate otherwise.

The ISPS Code and the USCG regulation provide a list of scenarios that should be combined with specific critical targets to develop the scenarios to be evaluated in the Port Security Assessment. Those scenarios include:

- Damage to, or destruction of, the port facility or of the ship (e.g., by explosive devices, arson, sabotage or vandalism)

- Hijacking or seizure of the ship or of persons on board
- Tampering with cargo, essential ship equipment, or systems or ship's stores
- Unauthorized access or use, including presence of stowaways
- Smuggling weapons or equipment, including weapons of mass destruction
- Use of the ship to carry those intending to cause a security incident and their equipment
- Use of the ship itself as a weapon or as a means to cause damage or destruction
- Blockage of port entrances, locks, approaches, etc.
- Nuclear, biological, and chemical attack

A target may prompt a few or many scenarios. The number of scenarios is left to the judgment of the PSA team. Care should be taken to avoid unnecessarily evaluating excessive numbers of similar scenarios or those that result in low consequences. That is why a criticality assessment should be performed initially to focus efforts on critical targets. Minor variations of the same scenario also do not need to be evaluated separately unless there are measurable differences in consequences or vulnerabilities.

### **STEP 3: CONDUCTING A CONSEQUENCE AND VULNERABILITY ASSESSMENT**

In this step each target/attack scenario combination is evaluated in terms of the potential consequences of the attack and the vulnerability (or invulnerability) of the target to the attack.

Five elements are included in the consequence assessment: death and injury, economic impact, environmental impact, national defense impact, and symbolic effect. Descriptions of the consequence components are provided in Table 2.

**Table 2 Consequence Categories and Descriptions**

<b>Category</b>	<b>Description</b>
Death and Injury	The prospective number of lives lost and injuries occurring as a result of an attack scenario.
Economic Impact	The potential economic impact of an attack scenario.
Environmental Impact	The potential environmental impact of an attack scenario.
Public Safety/Defense Impact	The potential effect on public safety/defense resulting from an attack scenario on different targets, including Department of Defense (DoD) targets.
Symbolic Effect	The potential that the target is closely linked as a symbol with the American economy, political system, military, or public welfare.

Individual consequence elements for a given scenario need to be addressed, but should be summarized into a single score for each target/scenario combination: high, medium, or low.

Consequence categories and criteria with benchmark examples are provided in Table 3. The PSA team can alter the scoring criteria in Table 4 to accurately reflect the physical characteristics and activity in the area being assessed (e.g., >100 deaths or serious injury versus >1,000 for a rating of high), but any changes and their rationale should be clearly documented.

**Table 3 Consequence Assessment Criteria**

	<b>Death/ Injury</b>	<b>Economic Impact</b>	<b>Environmental Impact</b>	<b>National Defense</b>	<b>Symbolic Effect</b>
<b>High</b>	>1,000 deaths or serious injuries	>\$U.S. 100 million	Complete destruction of multiple aspects of the ecosystem over a large area	Creates critical long-term vulnerabilities in public safety/defense	Major damage of nationally important symbols that are internationally recognized
<b>Medium</b>	100 to 1,000 deaths or serious injuries	From \$U.S. 10 to 100 million	Long-term damage to a portion of the ecosystem	Short-term disruptions in public safety/defense	Major damage or destruction of regionally or locally important symbols
<b>Low</b>	0 to 100 deaths or serious injuries	<\$U.S. 10 million	Small spills with minimal, localized impact on the ecosystem	No serious safety/defense impact	Minor/no damage to an important symbol

Four elements of vulnerability are included in the computation of the vulnerability score: availability, accessibility, organic security, and target hardness. Descriptions of the vulnerability components are presented in Table 4.

**Table 4 Vulnerability Categories**

<b>Category</b>	<b>Description</b>
Availability	The target’s presence and predictability as they relate to the ability to plan an attack.
Accessibility	Accessibility of the target to the attack scenario. This relates to physical and geographic barriers that deter the threat without organic security.
Organic Security	The ability of security personnel to deter the attack. It includes security plans, communication capabilities, guard force, intrusion detection systems, and timeliness of outside law enforcement to prevent the attack.
Target Hardness	The ability of the target to withstand the specific attack based on the complexity of target design and material construction characteristics.

The PSA committee or team should discuss each vulnerability element for a given scenario but should summarize the discussion into a single score for each target/scenario combination; high, medium, or low. The initial evaluation of vulnerability should be viewed *without* new strategies meant to lessen vulnerabilities, even if there are strategies already in place. For future reference, the organic security components already being used should be noted. Assessing the vulnerability without

strategies will provide a more accurate baseline score of the overall risk associated with the scenario. After the initial evaluation has been performed, a comparison evaluation can be made *with* new strategies considered. Vulnerability categories and criteria are provided in Table 5.

**Table 5 Vulnerability Assessment Criteria**

<b>Category</b>	<b>Availability</b>	<b>Accessibility</b>	<b>Organic Security</b>	<b>Target Hardness</b>
<b>High</b>	Always available (e.g., continually present or present daily on a set schedule)	No deterrence (e.g., unrestricted access to target and unrestricted internal movement)	No deterrence capability (e.g., no plan, no guard force, no emergency communication, outside L.E. [law enforcement] not available for timely prevention, no detection capability)	Intent of attack easily accomplished (e.g., readily damaged or destroyed)
<b>Medium</b>	Often available (e.g., present several times a month; arrival times predictable 1 week to 2 months in advance; predictable departure times)	Good deterrence (e.g., single substantial barrier; unrestricted access to within 100 yd of target)	Good deterrence capability (e.g., minimal security plan, some communications, armed guard force of limited size relative to the target; outside L.E. not available for timely prevention, limited detection systems)	Good ability to withstand attack (e.g., simple design but relatively strong construction)
<b>Low</b>	Rarely available (e.g., no set schedule and on any given day presence highly unlikely and unpredictable; arrives once a year or less for a few hours and arrival is not publicly known)	Excellent deterrence (expected to deter attack; access restricted to within 500 yd of target; multiple physical/geographical barriers)	Excellent deterrence capability expected to deter attack; covert security elements that represent additional elements not visible or apparent	Target expected to withstand attack (e.g., complex design and substantial construction of target minimizes success of attack)

## STEP 4: CATEGORIZING THE TARGET/SCENARIO COMBINATIONS

The team should next determine which scenarios should have mitigation strategies, identified by determining where the target/scenario combination falls in Table 6, based on the consequence and vulnerability assessment scores.

**Table 6 Vulnerability and Consequence Matrix**

		Vulnerability Score		
		Low	Medium	High
Consequence Score	High	Consider	Mitigate	Mitigate
	Medium	Document	Consider	Mitigate
	Low	Document	Document	Document

“**Mitigate**” means that mitigation strategies should be developed to reduce risk for that target/scenario combination. A security plan should contain the scenario evaluated, the results of the evaluation, and the mitigation measures.

“**Consider**” means that the target/scenario combination should be considered and mitigation strategies should be developed on a case-by-case basis. The Port Security Plan should contain the scenario evaluated, the results of the evaluation, and the reason mitigation measures were or were not chosen.

“**Document**” means that the target/scenario combination does not need a mitigation measure at this time, and therefore needs only to be documented. The security plan should contain the scenario evaluated and the results of the evaluation. This will be beneficial in further revisions of the security plan in order to know if the underlying assumptions have changed since the last edition of the security assessment.

## STEP 5: DETERMINING MITIGATION STRATEGIES AND IMPLEMENTATION METHODS

The true value of these assessments is realized when mitigation strategies are implemented to reduce consequences and vulnerabilities. The desire is to reduce the overall risk associated with the identified target/scenario combinations. Note that, generally, it is often easier to reduce vulnerabilities than to reduce consequences or threats when considering mitigation strategies.

As an example of a possible vulnerability mitigation measure, a company may contract for a standby tug to provide “sentry duty” to prevent ramming of a cruise ship. This measure would improve organic security and may reduce the overall vulnerability score from a “high” to a “medium.” However, this option is specific for this scenario and also carries a certain cost. Another option might

be to dock the cruise ship in a more protected berth. This may reduce the accessibility score from “high” to “medium.” This option may not require additional assets, but reduces the risk of this scenario, and may even provide mitigation for additional scenarios. Similarly, other scenarios can be tested to determine the most effective strategies.

A strategy may be thought of as effective if its implementation lowers the overall consequence or vulnerability score. A strategy may be thought of as partially effective if the strategy will lower an overall score when implemented along with one or more other strategies. A strategy may be thought of as having no effect if its implementation does not lower a score.

A strategy may be thought of as feasible if it can be implemented with little trouble or funding within current budgetary constraints. A strategy may be thought of as partially feasible if its implementation requires significant changes or additional funding. A strategy may be thought of as not feasible if its implementation is problematic or is cost prohibitive except under extreme threat conditions.

The PSA team should keep in mind that strategies must be deployed commensurate with various security threat levels established and set by the appropriate government agency. Effective strategies that are feasible should be considered for implementation at the lowest security threat level. Effective but partially feasible strategies may be implemented during higher security threat levels. Strategies must ultimately maintain, to the utmost, an equivalent level of security despite changes in security threat levels.

After the selection of the mitigation strategies and implementation methods, the PSA team should check the results to ensure that critical operations are maintained and the risk is reduced to the port. Some mitigation strategies might include shutting down noncritical operations during higher threats.

***APPENDIX 2***

***Example Port Facility Security Plan***

# ***FACILITY SECURITY PLAN***

## **Harbor Point Facility**

Version 1.0

September 2003

## **Harbor Point Facility**

**Operated by Harbor Point Operating Company**

**This is Controlled Document Number CDN-XXX and is not for general review. No copying or forwarding of this Plan is allowed without the express approval of the Facility Security Officer.**

*{Note: Because this is a generic plan rather than a Facility-specific plan, it is not marked as security sensitive information. Typically, port/port Facility Security Plans should be plainly marked to warn personnel having access to the plan that it needs to be protected and should not be released. In addition, companies need to coordinate with their port authorities to determine specific security information protection measures that apply.}*

## **TABLE OF CONTENTS**

DEFINITIONS.....	A2-6
SECTION 1 INTRODUCTION.....	A2-8
1.1 Purpose and Regulatory Basis .....	A2-8
1.2 Plan Security and Control.....	A2-8
1.3 Periodic Review and Audit of Procedures .....	A2-8
SECTION 2 PORT FACILITY DESCRIPTION.....	A2-10
SECTION 3 SECURITY ORGANIZATIONS.....	A2-11
3.1 Company Policy.....	A2-11
3.2 Facility Security Officer (FSO).....	A2-11
3.3 Ship Security Officer (SSO) .....	A2-12
3.4 Harbor Point Port Security Committee.....	A2-12
3.5 Emergency Services and Contracted Security Services .....	A2-12
SECTION 4 SECURITY TRAINING, DRILLS, AND EXERCISES.....	A2-14
4.1 General .....	A2-14
4.2 Security Awareness Program.....	A2-14
4.3 Security Training Courses/Exercises.....	A2-15
SECTION 5 PLANS, PROCEDURES, AND CONTROLS .....	A2-16
5.1 General .....	A2-16
5.2 Security Levels .....	A2-16
5.2.1 Security Level 1 .....	A2-16
5.2.2 Security Level 2.....	A2-16
5.2.3 Security Level 3.....	A2-17
5.3 Declaration of Security.....	A2-19
5.4 Access Control Plan .....	A2-19
5.4.1 General.....	A2-19
5.4.2 Security Guards .....	A2-19
5.4.3 Access Points to the Facility .....	A2-20
5.4.4 Restricted Areas .....	A2-20
5.5 Visitors ID .....	A2-21
5.5.1 General.....	A2-21
5.5.2 Administrative Requirements.....	A2-22
5.6 Vehicle ID .....	A2-22
5.7 Security Lighting Plan.....	A2-22
5.7.1 General.....	A2-22
5.7.2 Additional Information About the Security Lighting Plan .....	A2-22
5.8 Security Equipment and Systems .....	A2-23
5.8.1 Security Control Center (SCC) .....	A2-23
5.8.2 Security Systems and Equipment .....	A2-23
5.8.3 Intruder Detection and Alarm Systems.....	A2-25
5.8.4 Portable Security Equipment.....	A2-25
5.8.5 Equipment Responsibilities.....	A2-26

## **TABLE OF CONTENTS (cont'd)**

5.9 Facility Search Plan.....	A2-26
5.9.1 General.....	A2-26
5.9.2 Relative Search.....	A2-26
5.9.3 Preventive Search.....	A2-27
5.9.4 Unlocked and Locked Spaces .....	A2-27
5.9.5 Search Plan.....	A2-27
5.9.6 Conducting Searches .....	A2-27
5.9.7 Search Methods .....	A2-28
5.10 Personal/Individual Searches .....	A2-28
5.10.1 General.....	A2-28
5.10.2 Search Method.....	A2-28
5.11 Movement of Crew from or to a Ship Berthed at the Facility .....	A2-29
5.12 Ship's Stores and Unaccompanied Baggage.....	A2-29
5.13 Ship Bunkering, Waste Transfer, and Other Servicing Vessels.....	A2-30
5.14 Computer Security .....	A2-30
5.15 Locks and Keys.....	A2-30
5.15.1 General.....	A2-30
5.15.2 Master Keys .....	A2-30
5.15.3 Duplicate Keys .....	A2-31
5.15.4 Lost/Replacement Keys .....	A2-31
5.16 Availability of Facility Information .....	A2-31
5.16.1 Records/Reports .....	A2-31
5.16.2 Security Incident Reports.....	A2-32
5.17 Communications Equipment, Systems, and Protocols .....	A2-32
5.17.1 General.....	A2-32
5.17.2 Established Routine Communications for the Different Security Levels .....	A2-32
5.17.3 Communication with Vessels Alongside the Facility.....	A2-33
5.17.4 Duress Words and Codes .....	A2-33
5.17.5 Action Upon Hearing the Duress Word/Code.....	A2-34
5.17.6 Calibration, Testing, and Maintenance of Communications and Security Systems and Equipment .....	A2-34
<b>SECTION 6 PROCEDURES FOR RESPONDING TO SECURITY THREATS.....</b>	<b>A2-35</b>
6.1 General .....	A2-35
6.2 Weapons and Ammunition .....	A2-35
6.3 Use of Force.....	A2-35
6.3.1 General.....	A2-35
6.3.2 Basic Rule for Use of Force .....	A2-35
6.3.3 Security Objectives .....	A2-35
6.3.4 Limitations to the Use of Force.....	A2-36
6.4 Action on Receipt of a Bomb Threat.....	A2-36
6.4.1 General .....	A2-36
6.4.2 Bomb Threat Types .....	A2-37
6.4.3 Bomb Threat Analysis .....	A2-38
6.4.4 Bomb Threat Actions (Operational) .....	A2-38
6.5 Action on Discovery of a Bomb or a Suspect Package .....	A2-39
6.5.1 Policy Statement.....	A2-39
6.5.2 Bomb Discovery Response Procedure.....	A2-39

**TABLE OF CONTENTS (cont'd)**

6.6 Actual Explosion or Detonation..... A2-39  
6.7 Evacuation Procedure..... A2-39  
    6.7.1 General..... A2-39  
    6.7.2 Method of Communication ..... A2-39  
    6.7.3 Primary and Secondary Evacuation Routes ..... A2-40  
ANNEX 1 Approval Letter of Harbor Point Facility Security Plan..... A2-41  
ANNEX 2 Emergency Services and Key Contact Telephone Numbers List ..... A2-44  
ANNEX 3 Declaration of Security..... A2-46  
ANNEX 4 Personnel/Visitor Log Sheet ..... A2-49  
ANNEX 5 Telephonic Bomb/Threat Register Form..... A2-51  
ANNEX 6 Facility Security Plan and USCG Regulation Cross Reference..... A2-54

## ***DEFINITIONS***

**Captain of the Port (COTP):** means the Coast Guard officer designated by the Commandant to command a Captain of the Port Zone as described in 33 CFR Part 3, or their authorized representative. In other countries, this person may be called the Harbor Master, Port Master, or similar terminology.

**Commandant** means the Commandant of the U.S. Coast Guard as described in 46 CFR 1.01-05.

**Company Security Officer (CSO)** The company official from the ship operator who will be responsible for developing, maintaining and enforcing the company security policies as set out in this document.

**Declaration of Security: (DOS)** means an agreement to be executed between the responsible Vessel Security Officer and Facility Security Officer, and provides means for ensuring that the critical security concerns are properly address and security will remain in place throughout the time the vessel is moored at the facility. Security for the facility is properly addressed by delineating the responsibilities for security arrangements and procedures between a vessel and a facility.

**Drills and Exercises** means frequent and detailed training conducted by the port facility to ensure that personnel are proficient in all assigned security duties, at all security levels, and to identify any security related deficiencies, which need to be addressed. Exercises are comprehensive training events that involve most of the items noted in Section 3.3 of this plan. Drills more frequent but less comprehensive than exercises are to be used to maintain a high level of security readiness.

**Disembark:** Refers to any time that the crew or passengers leave the ship, be it a port call or final destination.

**Embark:** Refers to any time that crew or passengers board the ship, be it a port of call or initial boarding of the ship.

**Facility** means all contiguous structures or facilities located in, on, under, or adjacent to any waters of the United States.

**Facility Security Officer: (FSO)** means a person appointed as responsible for the development, implementation, revision, and maintenance of the Facility Security Plan, and to serve as the liaison with the Vessel Security Officer and company security officers.

**Facility Security Plan (FSP)** means a plan developed to ensure the application and measures designed to protect the facility and vessels, their cargoes, and persons on board from the risks of a security incident.

**Facility Security Assessment** means an analysis that examines and evaluates possible threats, vulnerabilities, and existing protective measures, procedures and operations.

**Maritime Security (MARSEC) Level 1 (Security Level 1)** means the level for which minimum appropriate protective measures must be maintained at all times.

**Maritime Security (MARSEC) Level 2 (Security Level 2)** means the level for which appropriate additional protective security measures will be maintained for a period of time as a result of heightened risk of a transportation security incident.

**Maritime Security (MARSEC) Level 3 (Security Level 3)** means the level for which further protective security measures shall be maintained for a limited period of time when a transport security incident is probable or imminent, although it may not be possible to identify the specific target.

**Operator:** The person, company, or government agency, or the representative of a company or government agency, which maintains operational control over a passenger ship or passenger terminal.

**Unlawful Act:** An act that is a felony under U.S. federal law, under the laws of the states where the ship is located, or under the laws of the country in which the ship is registered.

**Ship Security Officer (SSO):** The specific individual onboard the vessel who is accountable to the master for the security of the vessel, including implementation and maintenance of the vessel security plan and to serve as the liaison with the company security officer and the Facility Security Officer. The SSO is identified by name and position on the ships crew list and in the 96-hour advance notice of arrival (when applicable).

**Vessel Security Interface:** means the activities that occur when a vessel is directly and immediately affected by an action involving the movement of people, goods or the provisions of port services to or from the vessel.

## SECTION 1 INTRODUCTION

### 1.1 Purpose and Regulatory Basis

The purpose of this Facility Security Plan (FSP) is to contribute to the prevention of illegal acts against the Harbor Point port facility located at Harbor Point, Any Harbor, USA., including it's personnel, and vessels berthed alongside. It has been prepared in accordance with:

Chapter XI-2 of SOLAS 1974 and the International Ship and Port Security Code (ISPS Code)

### 1.2 Plan Security and Control

Authorized copies of this FSP must be controlled so that all authorized holders of the plan have the current revision. The Facility Security Officer (FSO) is responsible for issuing revisions to this plan. Significant changes to this plan must also be approved by government authorities prior to implementation by the Harbor Point Port Authority.

Distribution of this FSP must be controlled so that it is restricted to personnel who have a need to know for purposes of implementing or assessing the security plan for this port facility. The requirement to protect this information must be covered in security training sessions provided for company personnel. Also, all copies of this plan (both electronic and printed) should be marked as specified by the company security program. All transmittals of a copy of the information in this plan should include a warning statement that the information is sensitive and must be protected.

*{Note: The list of persons who maintain a copy of this plan should be developed and included in the FSP.}*

### 1.3 Periodic Review and Audit of Procedures

The Security Plan is a living document that will be revised when experience or changes require, such as:

- .1 if the Facility Security Assessment (PFSA) relating to the port facility is altered;
- .2 if an independent audit of the FSP or the Contracting Government's testing of the port facility security organization identifies failings in the organization or questions the continuing relevance of significant elements of the approved FSP;
- .3 following security incidents or threats thereof involving the port facility; and
- .4 following changes in ownership or operational control of the port facility.

The FSO can recommend appropriate amendments to the approved plan following any review of the plan. Amendments to the FSP proposed by others must be reviewed by the FSO, particularly those relating to:

- .1 proposed changes which could fundamentally alter the approach previously adopted to maintain the security of the port facility; and
- .2 the removal, alteration or replacement of permanent barriers, security and surveillance equipment and systems, etc., previously considered essential in maintaining the security of the port facility.

Internal audits of the Facility Security Plan and its effective implementation are carried out annually. Personnel conducting internal audits of the security activities, procedures and equipment specified in the plan or evaluating its implementation are independent of the activities.

*{Note: The FSP should clearly state how such independent audits will be accomplished.}*

### **Statement of Compliance**

This security plan along with the security assessment, complies with the regulations of SOLAS Chapter XI-2 and the ISPS Code. The plan has been reviewed by the appropriate government authority. A copy of the Statement of Compliance is found in Annex 1.

## SECTION 2 PORT FACILITY DESCRIPTION

*{Note: The FSP should include basic information describing activities conducted at the Facility and how they are performed (e.g., facility activities, operations, cargo handled, staffing, work schedules, etc.) including the location of the facility (i.e., country, state, city, port, etc.).}*

### Handling of Cargo and Ship Stores

Facility provides handling, storage, and distribution of bulk oil/chemicals as identified in US CFR <insert regulation/paragraph number> and <insert regulation/paragraph number>. Whereas containerized and break bulk-type cargoes provide different opportunities for criminal and terrorist activity, such threats as tampering with bulk liquid cargo tends to present less of a likelihood. Even so, there is increased likelihood that oil and chemicals might be targeted due to their flammable and potential toxic properties. Inventory of stock including location and identifying characteristics, is maintained by <insert position name/title>. The procedures governing handling, storage, and distribution are established and are referenced in the Harbor Point Facility Operations Manual.

## SECTION 3 SECURITY ORGANIZATION

The Harbor Point Facility security policy is an active and practical security management policy, incorporating a range of measures, including plans, procedures and guidelines, in order to safeguard Harbor Point Facility, employees, visitors, the facilities, ships and cargoes from terrorist or other criminal organizations.

### 3.1 Company Policy

Harbor Point Operating Company will:

- .1 Observe the International Laws and Regulations regarding maritime security and ensure they are covered in this Security Manual.
- .2 Continue to practice good management.
- .3 Safeguard employees, visitors, the facility, cargo and ships alongside.
- .4 Appoint and empower a suitably senior facility employee (normally the Head of Operations) as the Facility Security Officer FSO, to have overall responsibility for security at the facility and give support to fulfill these duties and responsibilities.
- .5 Have the security risk assessed taking into account the type of facility and nature of the vessels that interface with it.
- .6 Co-operate with the responsible authorities and act on their advice.
- .7 Promote security awareness among all employees.
- .8 Provide guidance and advice, primarily this document, to Facility Security Officers on the response to security threats and keep such guidance updated.
- .9 Establish a security element to the Crisis Management Structure, including Media and Family Information Plans.
- .10 Establish a reporting and recording system for incidents and forward that information to the authorities.
- .11 Recognize that additional security requirements may impose additional burdens on facility personnel.
- .12. Recognize that security objectives may compromise personnel safety objectives and to ensure that the two are balanced appropriately.
- .13. Support the FSO in his authority to make independent security decisions and when to ask for assistance where necessary

### 3.2 Facility Security Officer (FSO)

A FSO is designated for <insert facility name> facility. The duties of the FSO may be delegated to other qualified personnel, but the FSO is ultimately responsible for these duties. A person designated as the FSO may act as the FSO for one or more facilities, depending on the number or types of facilities a company operates. Where a person acts as the FSP for more than one facility, it should be clearly identified which facilities this person is responsible for, and be acceptable to the Contracting Government for the area in which those facilities operate. The FSO position may be collateral duty provided the person is fully capable to perform the duties and responsibilities required of the FSO.

The duties and responsibilities of the FSO should include, but are not limited to:

- .1 conducting an initial comprehensive (on-scene) security survey of the port facility taking into account the relevant port facility security assessment;
- .2 ensuring the development and maintenance of the Facility Security Plan;
- .3 implementing and exercising the Facility Security Plan;
- .4 undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;
- .5 recommending and incorporating, as appropriate, modifications to the Facility Security Plan in order to correct deficiencies and to update the plan to take into account relevant changes to the port facility;
- .6 enhancing security awareness and vigilance of the port facility personnel;
- .7 ensuring that security plans, procedures, systems and equipment do not compromise the personnel safety of facility employees, contractors, and visitors
- .8 ensuring adequate training has been provided to personnel responsible for the security of the port facility;
- .9 reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;
- .10 coordinating implementation of the Facility Security Plan with the appropriate Company and Ship Security Officer(s);
- .11 coordinating with security services, as appropriate;
- .12 ensuring that standards for personnel responsible for security of the port facility are met; and
- .13 ensuring that security equipment is properly operated, tested, calibrated, and maintained.

### **3.3 Ship Security Officer (SSO)**

A ship security officer SSO, will be designated on many of the ships that berth at this facility (i.e., when required by governmental authorities). Like the FSO, the SSO is responsible for implementation of the duties and procedures described in the vessel's ship security plan. The following SSO duties will impact ship-to-shore interface.

- .1 coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility;
- .2 coordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer;
- .3 assisting the FSO in confirming the identity of those seeking to board or disembark the ship when requested; and
- .4 assisting the FSO in confirming the identity of stores or other items intended to be placed onboard or removed from the ship.

### **3.4 Harbor Point Port Security Committee**

*{Note: Describe any port or regional organization, of which the facility is a member, that addresses security or mutual aid.}*

### **3.5 Emergency Services and Contracted Security Services**

The level of response required from emergency services must be determined after evaluation of a security incident has been completed by the FSO and other security personnel. In addition to

assistance that can be rendered by local police, firefighting services, and other government organizations, specialized teams may be contacted for bomb disposal, waterside patrols, and dive searches.

The specific companies that the Harbor Point Facility uses for contracted emergency response and security services are:

***{Note: Provide a list of such companies here.}***

Emergency and specialized services and other important contact details are listed in Annex 2, Emergency Services and Key Contact Telephone Numbers.

## **SECTION 4 SECURITY TRAINING, DRILLS, AND EXERCISES**

### **4.1 General**

Every employee has a security responsibility at all times. A continuous, vigorous and forceful facility security program must reinforce facility-wide security consciousness and awareness. The FSO shall establish and promote a security education program and will serve as the training coordinator for this program. This program shall ensure that all assigned personnel: recognize, understand, and are capable of performing their responsibilities regarding security. Security education must stress that security is everyone's business, and all personnel must understand their role in the facility physical security program.

The objectives of security training, drills, and exercises are to:

- .1 Encourage prompt reporting of security breaches.
- .2 Seek to eliminate security infractions and violations.
- .3 Enhance facility defenses against espionage, sabotage, and terrorist attack.
- .4 Provide feedback for improving protective measures.
- .5 Encourage employee reporting of security provisions that compromise employee/visitor's personnel safety.
- .6 Instill security consciousness that will solicit potential threat information.
- .7 Familiarize personnel with the procedures established in the Facility Security Plan, bomb threat response plan, and security list.
- .8 Advise all personnel of the prohibition against discussing classified information over unsecured telephones, radios, or in any manner that permits interception by unauthorized persons.
- .9 Inform all personnel of the penalties for engaging in industrial or national defense espionage activities and violations of security regulations.
- .10 Inform all personnel of the requirement to report any suspicious contact, however casual or seemingly innocent.
- .11 Educate security personnel in procedures and tactics to prevent and/or control intruders.
- .12 Ensure drills are performed every three months and exercises every calendar year (but not longer than 18 months between exercises).

### **4.2 Security Awareness Program**

All newly assigned personnel, regardless of position, shall be given a general security instruction (i.e., general security awareness orientation). The reading of printed security regulations alone is not sufficient to ensure understanding. Instruction will consist of an orientation on the need for, and dangers to, security and of the individual's responsibility. It shall include a discussion of security hazards common to all personnel, with emphasis on the danger of loose talk and operational carelessness. It shall define security measures in effect (e.g., visitor badge system, access control, patrol procedures, etc.). Additional instructions shall be provided to the degree commensurate to each individual's assignment and duties.

In order to ensure the proper state of readiness and proficiency, security training shall be conducted quarterly. All members of the facility's reaction force and other personnel, who may be required to perform security duties, shall participate in quarterly security training.

### 4.3 Security Training Courses/Exercises

Arrangements, schedules, performance, and personnel attendance at Security Training Courses is the responsibility of the FSO. The FSO will ensure that an exercise, that tests communications and response facts of the security plan, is carried out once every calendar year and not longer than 18 months between consecutive exercises.

**Table 1 Security Training, Drill, and Exercise Schedule**

Item	Involving	Frequency	Comments
<b>Training Sessions</b>			
Initial Security Awareness Training	Entire facility personnel	When initially assigned to facility	
Refresher Security Briefing	Entire facility personnel	Annually	
Security Plan Training	Selected facility members	When assigned Also when the plan is revised	Should include all personnel who have a role in implementing any action in the security plan
Facility Security Officer Training	All personnel that will assume the role of FSO	When assigned	Should cover regulatory basis for, and development/maintenance of, security plans
Security Staff Training	All personnel whose full-time job is a security function	When assigned	Can be modified based on the law enforcement/ security experience of the candidate
Bomb detection equipment	Personnel assigned to use the equipment	Prior to assignment	May be adequate to implement manufacturer provided procedures and training
<b>Drills</b>			
Bomb Threat/Bomb Search Drill	Bomb search personnel	Annually	Should also be covered in training when individuals are assigned to the facility
Security Level 3 Conditions	All security personnel	Annually	
Contraband Baggage Introduction (e.g. mock weapon)	Search team	Periodically based on equipment and procedures	Exercise should be conducted without prior knowledge of search
FSO – planned drill	Topic selected by FSO	Quarterly	This drill can be one of the drills defined above
<b>Exercises</b>			
FSO – planned exercise	Facility, contractors, and government authorities (if possible)	Annually (Not to exceed 18 months)	Can be combined with other exercises (e.g., spill response)

## SECTION 5 PLANS, PROCEDURES, AND CONTROLS

### 5.1 General

Security measures that have been established are implemented according to the Security Level that currently applies to the facility. The security level is decided by <insert organization firm> for the Contracting Government. In order that all security measures available to Harbor Point Facility (as determined in the Security Assessment) can be properly implemented, the FSO is responsible for maintaining a Security Roster that makes clear who is assigned to be responsible for carrying out specific security-related tasks and duties.

*{Note: The FSP should state that a copy of assigned Security Duties (the Security Duty Roster) is located at <insert location>. The FSP should also identify anticipated security duties for each of the three established Security (threat) Levels and personnel (position titles/names) assigned to perform each duty, including their 24-hour contact information.}*

### 5.2 Security Levels

There are three levels for Maritime Security at this facility. Security provisions listed below for each security level should be implemented in conjunction with requirements listed in Table 2.

#### 5.2.1 Security Level 1

This is the minimum security level. This threat level indicates a possibility of a (general) threat against facilities and shipping for which the security provisions for Threat Level 1 must be always maintained during normal working conditions.

- .1 Maintain 24 hour guard procedures.
- .2 Positively identify anyone accessing the facility (and their vehicles) for any reason.
- .3 Undertake searches of persons, personal effects, and vehicles.
- .4 Monitor 'Restricted Areas.'
- .5 Supervise cargo loading, including stored/staged cargo operations.
- .6 Require advance notice for arrival of ships; vehicles carrying stores, supplies, or repair items/replacement parts, and non-routine vendors/visitors.
- .7 Composition of stores, driver, and vehicle registration.
- .8 Search of stores/supplies delivery vehicle.
- .9 Ensure that communication is fully established with vessels/berthed along side.
- .10 Maintain a high situational awareness for suspicious activity.
- .11 Report any suspicious activity to the FSO/authorities.
- .12 Turn on appropriate lighting during hours of darkness.
- .13 Ensure all unused accesses are locked.

#### 5.2.2 Security Level 2

Security Level 2 is established when intelligence from a reliable source has been received indicating that a threat to ports/terminals has been given to a respective operating region, area, or port, or type of vessel, although no 'specific' target has been identified.

- .1 Assign additional personnel to guard access points and patrol perimeter barriers.

- .2 Pre-approve/screen in advance any persons requesting access to the facility.
- .3 Increase safeguards for ship stores to include coordination with SSO and escorts of vehicles.
- .4 Limit physical access to the facility and its sensitive areas (e.g., 'Restricted Areas')
- .5 Establish a Declaration of Security between vessel(s) and the facility.
- .6 Increase package/supply/stores screening.
- .7 Increase situational awareness for suspicious activity.
- .8 Verify the inventory of cargo in storage at the facility.

### 5.2.3 Security Level 3

Security Level 3 represents a high-level security threat against a specific target. This security threat level represents the highest threat level, based on reliable intelligence services, and indicates that a specific vessel or port facility has been identified as a 'target' and that the threat is highly probable or imminent.

- .1 Maximize use of lighting and surveillance equipment.
- .2 Prohibit non-essential access to the facility.
- .3 Secure all access points to the facility.
- .4 Consider ceasing all cargo handling/transfer operations.
- .5 Follow government authority and Company instructions regarding facility operations.
- .6 Revise ship schedules until the threat is eliminated.
- .7 Ensure that vessel(s) berthed along-side and/or entering or leaving the facility are informed.
- .8 Secure all barge hatches to prevent unauthorized cargo discharge.
- .9 Consider waterside surveillance.
- .10 Prepare to evacuate or partially evacuate the facility.
- .11 Implement specific/additional protective measure/actions ordered by the appropriate government authorities.

**Table 2 Security Level Requirements**

<i>Protective Measure</i>	<i>Security Level</i>		
	<b>1</b>	<b>2</b>	<b>3</b>
All facility personnel will review and exercise their security duties and responsibilities through drills, training, and exercises.	✓*	✓*	✓*
Provide security information to all facility and security personnel that addresses the security level and any specific threat information.	Optional	✓	✓
FSO will communicate with vessels along-side to coordinate protective measures.	✓	✓#	✓#
Security Manual is in place and implemented.	✓		
FSO and security personnel are assigned.	✓		
Facility Security Plan is written, revised, and working.	✓		
Restricted Areas are marked and monitored.	✓		
Access to Restricted Areas is denied contingent on normal safety.	✓		
Vulnerable points are locked.	✓		
Access is monitored and the personnel/visitor log is in order.	✓		
Unused accesses are secured.	✓		
Personnel and visitor IDs are worn.	✓		
Security equipment, lighting, and surveillance is operational.	✓		
Normal liaison with Port Security Committee is continued and Security Level status is acknowledged.	✓		
High situational awareness for suspicious activity is maintained.	✓		



### 5.3 Declaration of Security

Because the interface between vessel(s) and the Harbor Point Facility is critical to ensuring that appropriate security measures are maintained at all times for all security levels, and that neither the vessel or facility inhibits the level of security provided by the other, a security agreement between the vessel(s) and facility may be required. The agreement is called the Declaration of Security (DoS).

*Declaration of Security* means an agreement reached between a ship and a facility with which it interfaces, specifying the security measures each will implement. The DoS will be completed at Security Levels 2 and 3 and may also be provided at Security Level 1 depending on the cargo handled, specific government requirements, and/or Flag Administration requests.

When a DoS is mandated, it will be completed by the Master or the SSO on behalf of the ship and the FSO or, if the Contracting Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility. A copy of the DoS must be kept by both the ship and the port facility and shall be made available to government authorities upon request.

A sample DoS form is provided in Annex 3.

### 5.4 Access Control Plan

#### 5.4.1 General

Access Control is the key to basic physical security and is regulated by a number of measures laid out in paragraphs 5.4.2 through 5.6.

These measures are mandatory for the FSO to implement and uncontrolled or unescorted movement of any personnel will not be permitted. It should be emphasized that facility policy requires that:

- .1 A security watch is posted at all times.
- .2 All personnel and visitors must carry numbered and color-coded badges.
- .3 A personnel/visitor log is mandatory at all times.
- .4 Restricted Areas and Vulnerable Points are locked consistent with safety procedures.
- .5 Access regulations are coordinated with berthed and embarking/disembarking ship personnel.
- .6 Effective security lighting is maintained during periods of darkness.
- .7 The Access Control plan is documented and kept up-to-date.

The FSP has a drawn plan of the facility, which is annotated with:

- .1 all potential access points.
- .2 all Restricted Areas and Vulnerable Points.

#### 5.4.2 Security Guards

Qualified security personnel operate continuously to maintain access and traffic control, conduct perimeter and area surveillance, and form an intrinsic part of securing the facility during all Security Levels. Security personnel will report to the FSO all deficiencies found in lighting and

surveillance equipment as well as the occurrence of security incidents. Security personnel will also initiate emergency response for security and non-security related incidents.

*{Note: Biometric forms of personnel identification (ID) are currently under review for potential implementation. (This FSP will be updated if and when biometric ID systems are implemented.)}*

Security personnel are identified by their uniform appearance and photo identification card, which must be carried at all times. Additional persons will augment security personnel during increased Security Levels.

#### 5.4.3 Access Points to the Facility

Harbor Point Facility policy is that all unmonitored entrances remain closed unless they must be temporarily opened for operational reasons. Those that are opened must be monitored until they are resecured.

LIST EACH ENTRANCE *{Note: The FSP should list each entrance/gate by number or identifying code as indicated on the facility's diagram.}* REFER TO THE DIAGRAM OF RESTRICTED AREAS

Uncontrolled or unescorted movement must not be permitted. Therefore, a personnel/visitors 'gate' log is mandatory at all times. It shall show the current date, name of personnel/visitor, the firm represented, and vehicle registration. It shall also state the name of the person being visited, time in /out, and badge number.

An example Personnel/Visitor (Gate) Log Sheet is provided in Annex 4. On the 'gate log':

- .1 All entries must be made in ink.
- .2 Pages must never be torn out.
- .3 Mistakes must be corrected by drawing a line through the incorrect entry and placing initials next to the corrected information.

Each 'gate' log shall be retained for one year.

#### 5.4.4 Restricted Areas

Restricted Areas are to be marked (as below) and, provided that safety considerations are not compromised, shall be locked to prevent unauthorized access. This should certainly be the case at Security Levels Two and Three.

At Security Level 2, visitors should be escorted to Restricted Areas unless previously cleared and, at Security Level 3, access by visitors will be denied unless prior permission has been granted.

# WARNING

**RESTRICTED AREA - KEEP OUT  
AUTHORIZED PERSONNEL ONLY**

**AUTHORIZED ENTRY INTO THIS RESTRICTED AREA CONSTITUTES  
CONSENT TO SEARCH PERSONNEL AND THE PROPERTY UNDER  
THEIR CONTROL**

Areas designated to be 'restricted' include the:

- .1 Security Control Center
- .2 HVAC facilities and fan rooms.
- .3 Emergency power generator facilities and electrical contactor/switch rooms.
- .4 Battery and accumulator banks and spare stores.
- .5 Elevator machinery spaces.
- .6 Bottled gas stores.
- .7 Paint stores.
- .8 *{Note: Insert additional areas where personnel/visitor access must be secured and controlled at this facility.}*

## **5.5 Visitors ID**

### **5.5.1 General**

ID Badges will be color-coded and issued to Escorted or Non-Escorted repairmen or visitors. ID will only be issued on production of photographic identity documents. At Security Level 3, only pre-approved visitors will be allowed access to the facility.

Badges will be serialized (numbered) and color-coded as follows:

- .1 COLOR ONE: Visitor (business visitors/vendors) is on an approved, routine access list and an escort is not required.
- .2 COLOR TWO: Personal (personal/family visitors) visits. Sponsor will be responsible to escort visitor at all times.
- .3 COLOR THREE: Contract/other short-term or one-time visitors. A continuous escort is required and must be provided.

When large groups (i.e., service crews, stevedores, etc.) have their own badges, the team supervisor may sign in/out the entire crew.

Visitors who are issued badges will be told:

- .1 how the badge should be worn or displayed.
- .2 procedures to follow in case the badge is lost or stolen.
- .3 to return the badge upon termination of the visit and the location (gate/entrance) where it should be returned.

### 5.5.2 Administrative Requirements

All unused badges will be kept and maintained by the Facility Security Officer (FSO). Locally produced computer ID badges are acceptable, if serial-numbered and logged.

A badge inventory check is required and will be performed as follows:

- within 30 minutes after relieving a guard-watch.
- within 30 minutes by the guard-watch on duty after normal facility shift hours are completed.

Accountability of badges will be logged and discrepancies will be reported immediately to the FSO.

Lost badges will immediately be reported to the FSO for appropriate action.

## 5.6 **Vehicle ID**

All facility employee vehicles will be provided with a numbered windshield tag to allow for identification of the vehicle when unattended. Vehicles operated by visitors will be issued temporary passes at the gate access and will be restricted from parking at any location other than the visitor parking area, unless authorization to park in other areas is provided.

Random searches of vehicles will be made during Security Level 1 and 2. All vehicles will be searched during Security Level 3.

## 5.7 **Security Lighting Plan**

### 5.7.1 General

The primary purpose for any security lighting is to provide the means to detect and deter intruders.

Lighting implies human observation and will be ineffective if personnel are not present to observe illuminated areas. Proper security lighting is achieved by providing adequate uniform light along the perimeter, glaring light beyond the perimeter and into the eyes of intruders, and relatively little light along patrol routes or security posts. Darkness and periods of low visibility allow a perpetrator of criminal acts the potential for a higher degree of success. Therefore, modification of facility lighting may be required to impede, detect, and prevent a criminal act.

### 5.7.2 Additional Information about the Security Lighting Plan

- .1 Lighting will be provided along the perimeter of the facility including piers/wharfs. Lighting will be such that it will not cause a glare that hinders vision of security personnel or navigability of water traffic.
- .2 Light sources should be directed towards likely avenues of approach and/or the waterline to a minimum of 100 feet outwards from the perimeter of the onshore facility and piers and wharfs on the shoreside.

- .3 Lighting should provide overlapping illumination to prevent areas/dark spaces and should be continuous around the perimeter (waterside and shoreside) of all vessels that may be berthed at the facility simultaneously.
- .4 Security lighting will be activated during all hours of darkness.
- .5 Security vehicles must be equipped with spot lighting.
- .6 During Security level 2 and 3, temporary additional lighting will be established if any areas are not illuminated.

All deficiencies, or needed repairs, will be logged in and reported to the FSO immediately.

## **5.8 Security Equipment and Systems**

### **5.8.1 Security Control Center (SCC)**

The facility is equipped with a Security Control Center (SCC) due to security risks identified in the facility security assessment, the facility's size, and the complexity of its operations/activities. The SCC provides a secure/protected location for continuous (24-hour) monitoring of closed circuit television (CCTV) systems, intruder detection and alarm systems, and internal and external communications systems. In addition, portable and individual security equipment, including spares and reserves, are kept in the SCC when not in use. Security drawings, plans, and other security-sensitive documentation are secured in a dedicated vault/safe box located inside the SCC.

*{Note: Each port facility needs to (1) determine the need for a SCC at the facility and (2) develop and include information about the SCC (if provided in the FSP) on a case-by-case basis.}*

### **5.8.2 Security Systems and Equipment**

The facility utilizes the following security equipment and systems.

#### **Closed Circuit Television (CCTV) System**

Closed circuit television (CCTV) cameras will be provided in the areas indicated in Table 3:

**Table 3 Closed Circuit Television (CCTV) System**

<b>LOCATION</b>	<b>OBSERVATION</b>	<b>RECORDING FREQUENCY</b>	<b>NOTES/REMARKS</b>
Main Entrance (shoreside)	Access IN and OUT	24-Hour continuous	Recording kept on file in primary and back-up locations
Wharf Entrance(s)	Access IN and OUT	Continuous while vessels are berthed  Random at Security Level 1 or in accordance with Security Level 2 and 3 requirements	
Secondary, Auxiliary, and Emergency Access ways/Entrances and Egress Grates	Access IN and OUT	Random at Security Level 1 or in accordance with Security Level 2 and 3 requirements	
Perimeter (General)	Unauthorized encroachment	Random at Security Level 1 or in accordance with Security Level 2 and 3 requirements	
Perimeter (Culverts, Waterside Areas, and Other High Vulnerability Areas)	Unauthorized encroachment/access	Random at Security Level 1 or in accordance with Security Level 2 and 3 requirements	
Cargo/Stores Buildings	Unauthorized access/entry/activity	Continuous while personnel are present  Random at Security Level 1 or in accordance with Security Level 2 and 3 requirements	

**Table 3 Closed Circuit Television (CCTV) System (cont'd)**

LOCATION	OBSERVATION	RECORDING FREQUENCY	NOTES/REMARKS
Office Areas (Interior Space and Access ways), Entries, and Egress Doors	Unauthorized access/entry/activity	Continuous while personnel are present  Random at Security Level 1 or in accordance with Security Level 2 and 3 requirements	
Security Control Center (Interior and Entrance and Egress Doors)	Unauthorized access/entry/activity	24-Hour Continuous	

CCTV cameras/displays will be monitored on a continuous (24-hour) basis inside the Security Control Center.

5.8.3 Intruder Detection and Alarm Systems

A system of intruder alarms consisting of motion detectors and barrier-opening (secured gates and entry/egress doors) alarms are provided in accordance with the following table.

*{Note: A table similar to Table 3 for CCTV should be developed and inserted into the FSP at this location.}*

Intruder alarms will be monitored on a continuous (24-hour) basis inside the Security Control Center.

Fixed security equipment will be identified in a drawn plan of facility fence lines, access areas, lighting, restricted areas, parking, location of drains, culverts, rooftops, and other areas subject to continuous or random surveillance, etc.

5.8.4 Portable Security Equipment

*{Note: The list provided here is an example only and assumes that a professional security staff is onsite and trained in the use of this equipment. Replace this list with one that applies to your facility.}*

The following portable and individual equipment is provided at the facility

- .1 Hand-held metal detectors
- .2 Radiological material detectors
- .3 Gas detectors
- .4 Plastic explosive/bomb sniffing equipment

- .5 Blast blanket
- .6 Handcuffs, plasticuffs (band-type restraints for wrists and ankles)
- .7 Batons
- .8 Individual Security Equipment
- .9 Hand-held radio
- .10 Flashlight (torch)
- .11 Whistle
- .12 Pepper spray
- .13 Bull horn (if required)
- .14 Firearms (if temporarily brought into the facility during elevated security levels. See Section 6.2.)

#### 5.8.5 Equipment Responsibilities

The FSO is responsible for ensuring that:

- .1 Security personnel hold the correct equipment.
- .2 All equipment is in a workable state, tested, and calibrated.
- .3 Equipment is in good repair, maintained, and replaced as needed.
- .4 Appropriate supplies of reserve/replacement equipment are determined and provided.
- .5 Suggestions are reviewed regarding equipment utilization and types of equipment.

Personnel that are issued security-related equipment will ensure that:

- .1 Equipment is readily available
- .2 Equipment is secured in accordance with facility/company procedures and recognized good practices.
- .3 Equipment is in good order.
- .4 Equipment losses, breakage, and disrepair are reported to the FSO.

### 5.9 **Facility Search Plan**

#### 5.9.1 General

To ensure that a thorough and efficient search can be completed in the shortest possible time, search plans must be prepared and drilled. Search plans should be comprehensive and present logical routes for searchers to take into the areas they should search. The best way to do this is with a series of drill/practice cards that task individual searchers. Once a search task has been performed/drilled successfully, it can be ticked off a central tasking sheet. Practice search drills should be rotated across all work shifts and work crews at the facility to ensure that personnel, who need to be involved in conducting and supervising searches, have been drilled.

There are two types and two methods of conducting facility searches:

#### 5.9.2 Reactive Search

A reactive search is a search carried out in response to a specific threat or intelligence information. To be successful, a reactive search must include the following:

- .1 searchers who are familiar with the area and can notice unusual conditions or suspicious people or acts.
- .2 searchers must be able to recognize a bomb or other destructive or injurious device.
- .3 searchers must know what to do if a suspect device or person is found.
- .4 planning and control from/with a central reporting point.
- .5 searchers must have communications with central control.
- .6 a system of recording “clear” areas.

### 5.9.3 Preventive Search

A preventive search is aimed at anyone potentially smuggling a device into the facility. This will involve the search of all items before they are transported into the facility and must include crew, repairmen, facility staff, and visitors. It will also cover stores and provisions, trash, spares, and any other items coming into the facility either for the facility or for a vessel berthed at the facility.

### 5.9.4 Unlocked and Locked Spaces

When searching unlocked and locked spaces, the first response is to search all unlocked spaces followed by locked spaces.

### 5.9.5 Search Plan

So that searches can be implemented rapidly and thoroughly, the FSO must establish pre-threat search plans and ensure that ordered searches conform to the designated Search Plan. The plan needs to include:

- .1 a plan drawing of the facility.
- .2 ranking facility areas in priority-order for conducting sequenced searches, beginning with the most critical areas.
- .3 cards that cover each area of the whole facility to be searched. Cards should be distinguished by Stage One – Unlocked Areas and Stage Two – Locked Areas.
- .4 a central checklist covering all the cards for use by the search controller (i.e., FSO).
- .5 facility personnel should be designated to search specific areas; preferably their work area using a card for each designated area.
- .6 designation of personnel having the duty to communicate and coordinate facility searches with the Master or Ship Security Officer (SSO) of vessels berthed at, or on approach to, the facility.

### 5.9.6 Conducting Searches

Once a search is ordered, the FSO will centrally locate and brief search personnel on any relevant (threat) information received and also on how the search will be conducted. The briefing must address:

- .1 the type of search to be conducted – unlocked or locked, or both.
- .2 assignment of search personnel and distribution of search cards for allocation of areas of responsibility.
- .3 the priority of search areas and search activities.
- .4 the use and allocation of specialized security and/or detection equipment.
- .5 communications and control procedures/protocols.
- .6 coordination with attendant vessel Masters or SSOs.

## **DO NOT TOUCH ANY SUSPICIOUS OBJECT—REPORT ALL FINDINGS IMMEDIATELY**

### 5.9.7 Search Methods

When searching, assigned search personnel should:

- .1 Start from lower floors/levels of structures and work up.
- .2 Search from the outside/perimeter to the center of a space.
- .3 Avoid conducting random searches, or spot-checking logical threat areas, when conducting a detailed search.
- .4 Thoroughly check trash receptacles, storm water drains and culverts, and other enclosures/containers when searching outdoor areas.
- .5 Personnel familiar with machinery, utility, and other specialized spaces shall conduct searches of these areas. Attention should be given to locations where detonation devices could be placed to damage critical utilities such as electric power supply/distribution systems or equipment containing hazardous materials.
- .6 Have the occupants of the space stand by to open lockers, desks, cabinets, and other storage facilities and containers.
- .7 Upon orders from the FSO, be ready to coordinate their activities with Masters or SSOs of vessels berthed at or approaching the facility.

### **5.10 Personal/Individual Searches**

#### 5.10.1 General

The search of individuals constitutes the most stringent means of screening personnel and should be conducted at random at Security Level Two and should be mandatory at Security Level Three. Personal searches are normally conducted to prevent the introduction of illegal or unauthorized articles into the facility. When used, a search of individuals is a conditional requirement for entry into the facility. A person refusing the search shall be denied access and turned away. A search in progress should be stopped and the incident and person's identity reported immediately to the FSO and relevant authorities.

#### 5.10.2 Search Method

The intensity of personal search procedures to be implemented is the prerogative of the FSO. At Security Level One, a cursory "eyeball" examination may be sufficient. At Security Level 2, random searches and inspections of packages are required. The frequency of random searches (e.g., every third person, every tenth person) will be determined by the FSO and no personnel shall be exempt from search. At Security Level 3, a full search of every person and their property (e.g., packages, tools, vehicles, luggage, etc.) is mandatory. Once a decision is made to institute search procedures, the FSO shall consider the following methods of search:

- .1 Observe each visitor and checked items in the visitor's possession.
- .2 Use a metal detector to conduct an external body search.
- .3 Request each visitor to open vehicles and carry-in supplies, tools, and other items for examination.
- .4 Request each visitor to display any personal items hidden from view.
- .5 Request each visitor to display the contents of closed parcels and baggage/luggage.

- .6 Request visitors having electronic items (e.g., cell phones, calculators, portable/laptop computers, personal data appliances [PDAs], and other specialized portable electronic devices) to present such items for sequential screening actions in the following order:
  - (1) x-ray screening,
  - (2) having power to the electronic device turned on by the owner/holder of the device,
  - (3) confirmation by the facility searcher(s) that each electronic device appears to function properly.
- .7 Request each visitor to turn over any prohibited items for safekeeping until his/her departure from the facility.

Illegal, prohibited, and questionable (i.e., non-functional electronic devices and other suspicious items/materials) articles should be immediately brought to the attention of the FSO for further evaluation and/or disposal as appropriate.

### **5.11 Movement of Crew from or to a Ship Berthed at the Facility**

Ship crews may be relieved at the end of an extended period onboard or require temporary shore leave in order to complete recreational or other personal business. It is the policy of this facility to allow for the transit of ship crews between the vessel and the shore under control of facility personnel or other approved persons such as the ship's agent. No crew will be allowed to transit through the terminal without prior arrangement between the SSO and FSO. All ships' crew will be escorted to and from the access point. The FSO may determine that all such movement of crews is suspended if Security Level 2 or 3 are activated.

Ship agents or other authorized persons that facilitate the exchange of ship crews will be required to pre-arrange for transit through the facility with approval of the FSO. All crew and baggage will be subject to search. These conditions will be specified in the Declaration of Security.

### **5.12 Ship's Stores and Unaccompanied Baggage**

*Ship stores will not be allowed to pass across the facility at Security Level 3.*

Ships stores will normally be accepted through the facility for loading onto a vessel berthed alongside. Since the Ship Security Plan (SSP) for each vessel will have specific requirements for verification and search of stores, the opportunity to streamline the facility and vessel requirements should be considered to avoid unnecessary delay.

All stores for delivery to the vessel will be denied access unless prior notice is provided by the ship or the ship's agent. Notice must include description of the stores, packages, and package markings. Any deficiencies in the packaging will be noted on the stores list. The vehicle driver and registration must be provided in advance. On arrival, Gate Security will verify the vehicle and driver details and then notify the SSO, who will arrange to coordinate appropriate security requirements and have crew members meet the vehicle at the staging area. The stores vehicle will then be escorted to the designated vehicle staging area located at <insert location>. This area has been selected to be clear of all restricted areas and is separated from restricted areas by appropriate physical barriers.

When the stores vehicle is cleared for delivery, it will be escorted to the ship-side for unloading. The vehicle will not be allowed to move without facility escort.

Unaccompanied baggage will not normally be accepted by the facility. If due to exceptional circumstances, there is a requirement for baggage to be delivered, the requirements provided for ship stores will apply.

### 5.13 Ship Bunkering, Waste Transfer, and Other Servicing Vessels

*{Note: Servicing vessels that interface directly with port facilities are not likely to be covered by the ISPS Code or the USCG Maritime Security Regulations. Such non-ISPS Code, non-regulated vessels may introduce security risks to the facility if they transfer material or people to or from the facility. Such non-code/non-regulated vessels may include, but are not limited to, vessels that transport ship pilots or other personnel; vessels that bunker ship fuel, oils/lubricants, or potable water; vessels that transfer/accept ship based sanitary and hazardous liquid wastes; or vessels that transfer ship cargo, stores, or solid wastes.}*

*The FSP for the facility should address how facility security risks involving such vessels are assessed and managed. This will typically require coordination between facility security personnel, facility and ship operations personnel, and services vessel companies.}*

### 5.14 Computer Security

The electronic passage of information is subject to interception. Those not authorized to receive electronic information can read any material that is of a sensitive nature. Therefore, the following basic security precautions are required:

- .1 All computers must be identified for security purposes.
- .2 All computers must be password protected.
- .3 Back-up files must be securely maintained.
- .4 No unauthorized personnel will be allowed access to the facility computer system(s).
- .5 Storage of computer disks or other electronic recording media storing the FSP in electronic format must be secured at all times.

### 5.15 Locks and Keys

#### 5.15.1 General

*{Note: The FSP should include instructions or a procedure for distribution of keys, to assigned employee; substitution of locks when work/crew shifts change, when facility or contractor employees lose keys, or when their employment has been terminated or ends; as well as full replacement of locks and keys on a periodic basis.}*

#### 5.15.2 Master Keys

Master keys are to be held by:

- XXXX <insert position title/name >
- XXXX <insert position title/name >
- XXXX <insert position title/name >

### 5.15.3 Duplicate Keys

Any duplication of facility keys must be authorized in writing by the FSO.

### 5.15.4 Lost/Replacement Keys

All lost keys that need replacing will be reported to the FSO. The FSO will determine whether locks associated with lost keys must be replaced.

## 5.16 **Availability of Facility Information**

To assist in response and management of a crisis, basic facility information must be available for quick and effective reference. The FSO is responsible for ensuring that the information is revised, updated, and secured. The information should consist of at least the following items:

- .1 a large scale plan of the facility layout showing restricted areas, access points, lighting detail, and surveillance equipment.
- .2 a copy of this FSP
- .3 the name of the FSO and other key personnel (by assignments and duties)
- .4 current (valid) Declarations of Security.
- .5 names of facility personnel and their security responsibilities
- .6 a record of all means of communication.

This information shall be kept in a secure room, vault or safe box located in the Security Control Center (SCC), or an equally secure area, as addressed in Section 5.8 of this FSP.

### 5.16.1 Records/Reports

The following is the consolidated list of records required to be held by the FSO:

- .1 a copy of the Facility Security Assessment (FSA).
- .2 a copy of the Statement of Compliance for the Facility, issued by the Contracting Government.
- .3 a list of all vessels that have docked at the facility
- .4 Gate log entries.
- .5 Declaration of Security Record (log)
- .6 names of facility personnel and their security responsibilities.
- .7 dates and specifics of quarterly drills and annual exercises.
- .8 security incident reports, including breaches of security and any security incidents related directly to the facility and incidents involving a ship alongside, or service vessel.
- .9 changes in Security Levels.
- .10 on-scene surveys and inspections/verifications.
- .11 internal audits and reviews of security activities
- .12 reviews of FSA and FSP implementation
- .13 security measures in effect and their purpose.
- .14 security training, drill, and exercise records, including a roster of employees and contractors in attendance and the dates when conducted.
- .15 calibration, testing, and maintenance records for the Communications and Security Equipment

***{Note: The FSO shall determine and document the retention period applicable to each of the listed records in accordance with code and regulatory requirements and good practices.}***

#### 5.16.2 Security Incident Reports

It is required that all occurrences or suspected occurrences of unlawful acts and serious security breaches (violations) be reported to the FSO and that a report is forwarded, with necessary supporting information, to the appropriate authority, including the Contracting Government. This will include reporting all occurrences or suspected occurrences of unlawful acts committed onboard any vessel while berthed at the facility.

The FSO will keep all written Security Reports.

***{Note: Specific requirements of the Contracting Government will be listed here. The FSP shall also define a “serious breach (violation) of security.”}***

### 5.17 **Communications Equipment, Systems, and Protocols**

#### 5.17.1 General

The facility has the following communications equipment:

- .1 telephone from all offices, Security Control Center, storage warehouse, workshop, and guard locations.
- .2 pay phones located at <insert locations>.
- .3 company issued cell phones to the following personnel positions: <insert position titles>.
- .4 fax machines located at <insert locations>.
- .5 hand-held VHF and UHF radios issued to the following personnel positions: <insert position titles>.
- .6 e-mail from all office PC’s.
- .7 if the fire alarm is activated, automated response is initiated with the Fire Department.

All personnel that have been designated with security responsibilities will be provided hand-held radios. All radio traffic will be made on Channel <insert radio channel>. The backup Channel is Channel <insert radio channel>.

An alert system has been established to rapidly promulgate initial notice and status of security events to the Port Security Committee and other facilities in the area. ***{Note: The FSP should include a list of government agencies, nearby facilities, and pertinent contractors, along with the means to contact each.}***

#### 5.17.2 Established Routine Communications for the Different Security Levels

##### Security Level 1

- .1 established radio communication routine for facility-to-vessel reporting using hand-held, telephone, and VHF radio. Backup is established. Master’s cell phone number is with the Security Control Center.
- .2 established routine for communication with ships’ agent for scheduling/attending to crew changes and stores.

- .3 established routine for communication to the Port Security Committee and Contracting Government's Designated Authority.
- .4 established routine for communication to local police, the Fire Department, and other emergency services.

#### Security Level 2

- .1 increased frequency of facility-to-ship reporting.
- .2 increased reporting from access control points and patrols.

#### Security Level 3

In addition to Security Level 2:

- .1 Monitor channels for instructions from Port Security Committee/Contracting Government's Designated Authority.

#### 5.17.3 Communication with Vessels Alongside the Facility

Normal operations for transferring cargo to vessels berthed alongside utilizes UHF hand-held radios operated by the ship's Officer on-deck and the facility cargo supervisor and/or pump operator. Additionally, the ships' agent provides the Master a cell phone on arrival. The number for the cell phone is provided to the Security Control Center prior to commencing cargo operations and should be used for emergency purposes only.

*{Note: Facility procedures need to be developed to address these operational activities.}*

#### 5.17.4 Duress Words and Codes

Facility personnel that have been delegated security responsibilities will, as a matter of routine, implement and use a Duress Word/Code System to quietly announce a person in distress or a serious breach of security. This Duress Word/Code will be implemented in the following ways:

A Duress Word may be passed from a person in any fashion (i.e., the general announcing *system, hand-held radio, in person, etc.*). Associated personnel must know the active Duress Word/Code and know what actions to take should it be announced. The Duress Word will be changed whenever the Word has been compromised or deemed inappropriate. It will not be written down.

The FSO will:

- .1 Establish a procedure or protocol for managing situations when the Duress System is put into effect.
- .2 Ensure that all personnel are familiar with the Duress System protocol and active Duress Word/Code.
- .3 Conduct periodic training and drills in reaction to the covert Duress procedures.
- .4 Change the Duress Word or Code as required.

5.17.5 Action Upon Hearing the Duress Word/Code

Upon hearing the Duress Word or Code used by any person within the Facility, personnel will covertly inform the FSO and other security staff by the most expeditious (*but covert*) means that there is a security incident.

The FSO will initiate the appropriate level of response, including changing security levels and specifying required actions, in accordance with Section 6 of this plan (and associated procedures) based on the type of action deemed necessary.

5.17.6 Calibration, Testing, and Maintenance of Communications and Security Systems and Equipment

*{Note: This section should contain a list of all pertinent communications and security equipment, along with a schedule for any required calibration, testing, or preventive maintenance activities.}*

## SECTION 6 PROCEDURES FOR RESPONDING TO SECURITY THREATS

### 6.1 General

Any act or condition that may result in damage, loss or destruction of property, loss of life or disruption of the facility's mission is a threat.

A single individual, a small group, or a paramilitary or military force may initiate a threat. The minimum physical security standards in this plan are provided primarily in response to a threat imposed by a single individual or a small group who might attempt to attack the facility or board a vessel berthed alongside the facility.

### 6.2 Weapons and Ammunition

Facility policy states that no weapons or munitions are permitted within the facility (other than authorized law enforcement or other government agencies). Occasions may arise in response to specific security threats when government authorities order the placement of small arms and other portable weapons in a secure location in the facility. If this order is given, such weapons and ammunition shall be secured in the Security Control Center or other designated secure area.

### 6.3 Use of Force

#### 6.3.1 General

Personnel are entitled to exercise the right of self-defense in response to hostile acts or hostile intent. This is true both in times of peace and during armed conflict. In a peacetime environment, an actual or threatened imminent attack may be deflected by the application of force to the extent necessary and appropriate to terminate or forestall the attack, where no reasonable alternative is available. Furthermore, the facility and its security personnel need not wait to experience an actual attack prior to responding in self-defense. Anticipatory measures that are appropriate to forestall a clearly imminent attack are permitted under international law.

#### 6.3.2 Basic Rule for Use of Force

Personnel engaged in security activities will avoid the use of force when their assigned responsibilities can be discharged without resort to its use. However, if security responsibilities cannot be discharged without resort to the use of force, personnel shall use the minimum amount of force necessary to discharge their assigned responsibilities and to achieve their established security objectives.

#### 6.3.3 Security Objectives

The following hierarchy establishes appropriate levels of force in the order in which they should be applied and details the methods and tactics to be utilized in achieving the various levels of force:

- .1 *Verbal Command.* The verbal command is the ideal method of control since it results in the desired degree of control with no physical effort being exerted, and minimizes the prospect of

physical injury. A problem arises when the facility is faced with controlling non-facility personnel and members of the public who believe they are not subject to facility orders and whose objective is to willfully assault the facility and its personnel. In these instances the verbal command is usually ineffective.

.2 *Physical Force.* Direct physical contact is not a very effective application of force since the outcome is never certain. For this reason, the facility's security personnel should avoid actual physical contact except as required for searching or other controlled evolutions. One-on-one contact must be avoided unless it is required by a surprise situation. The security force member should protect himself/herself until he/she can back away, and then proceed to the next higher level of force required to control the attacking individual (such as restraining the individual with handcuffs and/or plastic cuffs on wrists and ankles). Once the resisting individual is restrained, the use of physical force will be confined to assisting the movement of the individual from one location to another. The available means of physical force are:

- *Physical barriers.* Physical barriers such as locked doors or confinement pens, will restrict movement and can be used to prevent an outsider from reaching his/her objective.
- *Fire Hose.* The use of a fully charged fire hose putting forth a solid stream of water can be a very effective application of physical force that avoids direct contact during the early phase of an intruder's attempt to gain entry to the facility.
- *Chemical Agent Control.* The common chemical control agent used by security personnel is identified as OC (Oleo Capsicum) or "pepper spray". The effect of this agent is temporary in nature, lasting no longer than 15 or 20 minutes. This amount of time is generally enough to gain physical control of the individual, or group, and to apply restraining devices. OC is classified as non-lethal, since there are generally no significant after-effects when properly used. Physiological effects are immediate and there is a high margin of safety. The use of chemical control agents should always be considered early in a confrontational situation where the intruding/offending party is advancing on a member of the facility security force. It will usually stop the assault for the period of time mentioned above, which may allow sufficient time to restrain the intruder(s) and issue appropriate security alerts called for elsewhere in this plan.

#### 6.3.4 Limitations to the Use of Force

This guidance is applicable only for the facility physical security measures taken pursuant to the implementation of the provisions of this plan. This guidance does not direct any violation of contract terms between facility owners/operators, or between facility owner/operators and personnel unions, or of any personnel contracts of employment. If this guidance conflicts in any way with such contracts or articles, or U.S. or host-country law, the contract, articles, or law will take precedence and this guidance will be null in-so-far as conflict is evident.

### 6.4 **Action on Receipt of a Bomb Threat**

#### 6.4.1 General

Every bomb threat will be taken seriously and the response will be immediate and systematic. This section increases the awareness of bombs and bomb threat conditions, as well as establishing the responsibilities and procedures the facility will implement when a bomb threat is received.

#### 6.4.2 Bomb Threat Types:

*Bomb Threat Notification.* Any individual at the facility who has received a bomb threat will immediately notify the FSO. Upon notification, the FSO will designate a person as the Bomb Scene Officer (BSO). This individual will then notify contacts of the all relevant agencies listed in Annex 2.

*Package and Mail Bombs.* The outward appearance of a package or mail bomb is limited only by the imagination of the sender. However, these bombs have exhibited the following unique characteristics that may assist facility personnel in identifying a suspected package or letter:

- .1 Mail bombs may bear restricted endorsements such as “personal” or “private”.
- .2 The addressee’s name and/or title may be inaccurate.
- .3 Mail bombs may reflect distorted handwriting or the name and address may be prepared with homemade labels or cut-and-paste lettering.
- .4 Package or mail bombs may have protruding wire, aluminum foil, or oil stains visible and may emit a peculiar odor.
- .5 Mail bombs may have an excessive amount of postage stamps affixed.
- .6 Letter-type bombs may feel rigid or appear uneven, or lopsided.
- .7 Parcel bombs may be unprofessionally wrapped and endorsed, “Fragile – Handle with Care” or “Rush – Do Not Delay”, or similar instructions.
- .8 Package or parcel bombs may have an irregular shape, soft spots, or bulges.
- .9 Package or parcel bombs may make a buzzing, ticking noise, or a sloshing sound.
- .10 Pressure or resistance may be noted when removing contents from an envelope or package.

*Telephone Bomb Threats.* There are two reasonable explanations for a caller reporting that a bomb will go off at a particular time.

- .1 The caller has definite knowledge or believes that an explosive or incendiary device has been, or will be, placed and the caller wants to minimize personal injury or property damage. The caller may be the person who placed the device, or someone who has become aware of such information.
- .2 The caller wants to create an atmosphere of anxiety and disrupt the normal routine, even though they are not aware of any actual bomb.

Personnel should respond calmly to a bomb threat call. If possible, get more than one person to listen to the call. Keep the caller on the line as long as possible. Ask the caller to repeat the message. Use the Telephonic Bomb/Threat Register Form (Annex 5) to record specific information related to a telephone call advising of a bomb threat.

In particular, the person receiving the call should:

- .1 Remain calm. Rarely has a bomb threat caller failed to allow ample time for evacuation.
- .2 Listen for voices or speech peculiarities and try to distinguish background noises that might help identify or locate the caller.
- .3 Be alert for repeated use of certain words or phrases.
- .4 Listen for national or regional accents.
- .5 Tape-record the conversation if possible.
- .6 Record the date and precise time the threat is received.
- .7 Try to get the caller to answer as many questions on the Telephonic Bomb/Threat Register Form as possible.

When the caller has answered the above questions, or refuses to do so, the person receiving the call shall notify the FSO. If possible, provide the location of the bomb and the time the caller stated it will detonate.

*Written Bomb Threats.* Save all materials, including any envelope or container when a written bomb threat is received. Once the message is recognized as a bomb threat, unnecessary handling should be avoided. Every possible effort must be made to retain evidence such as fingerprints, handwriting or typewriting, paper, and postal marks, as they are essential for tracing the threat and identifying the writer. While written messages are usually associated with generalized threats or extortion attempts, a written warning of a specific device may occasionally be received; it should never be ignored.

#### 6.4.3 Bomb Threat Analysis

In an attempt to determine whether or not a threat is real, the FSO shall call a meeting with the 'Heads of Departments' and review certain factors that could be considered predictive in nature. These factors include, but are not limited to:

- .1 determining the recent and current security posture (level and readiness) of the facility.
- .2 asking indicating questions, such as:
  - Were there any unidentified or unescorted intruders or suspicious acting visitors prior to the threat?
  - Were stores, cargo, mail, spare parts, or new equipment taken into, or through, the facility prior to the threat?
  - Has there been any recent dissension or unrest among facility personnel? Are there any disgruntled employees or contractors?
  - Has there been recent activity by activist groups or terrorist organizations?
- .3 conducting a risk evaluation related to vessels berthed alongside, or approaching or departing, the facility and evaluating their recent ports of call.

#### 6.4.4 Bomb Threat Actions (Operational)

When a threat is received, the FSO shall take the following operational actions as appropriate:

- .1 Consider ceasing operations.
- .2 Disconnect loading arms and hoses at the vessel and secure transfer systems.
- .3 Secure tanks.
- .4 Prepare to activate fire water systems.
- .5 Prepare to assist berthed vessels to depart.
- .6 Inform the appropriate maritime security authorities and comply with pertinent instructions/requirements.
- .7 Inform local police, the Bomb Disposal Unit, state and federal intelligence officers, and firefighting and emergency services.
- .8 Inform the SSOs of approaching vessels.
- .9 Prepare to evacuate the facility.

## **6.5 Action on Discovery of a Bomb or a Suspect Package**

### **6.5.1 Policy Statement**

Facility policy states that under no circumstances will anyone touch or remove a suspicious package that may contain a bomb or other destructive device. When a suspect package is found, it should be reported immediately to the FSO, giving a brief description if possible. Then follow the procedure/guidelines below.

### **6.5.2 Bomb Discovery Response Procedure**

*{Note: This section should provide a procedure developed by the facility in conjunction with local authorities such as the local police, fire department, and Bomb Disposal Unit.}*

## **6.6 Actual Explosion or Detonation**

In the event that an incendiary device has been detonated/exploded, the primary concern is for preserving life and assisting those who are injured. At this point, assembly and a headcount should be made of all personnel and evacuation of the facility ordered. Modification of the assembly points for personnel and the initiation of emergency response by trained facility personnel will be conducted according to the Emergency Plan.

Bomb Disposal Units are trained to provide additional consideration to secondary devices that are sometimes set by terrorist groups. Such devices are designed to detonate after the primary device has caused emergency services and first responders to be on-scene with the intent of causing additional injury/loss of life.

## **6.7 Evacuation Procedure**

### **6.7.1 General**

Evacuation of the facility will commence only when the FSO is satisfied that the information received is credible or when acting under the instruction of recognized crisis/emergency management and/or law enforcement authorities.

### **6.7.2 Method of Communication**

The FSO will alert personnel by the activation of the fire alarm, thereby initiating the assembly of, and accounting for, all personnel located within the facility, including ships personnel and visitors. The Personnel/Visitor Log Sheet (Annex 4) will be incorporated into the system of checking personnel and vehicles that are located within the facility.

Communication with facility personnel and SSOs will be conducted through the use of hand-held radios.

*{Note: Insert additional requirements of the Contracting Government or their Designated Authorities as necessary to fully address evacuation requirements.}*

### 6.7.3 Primary and Secondary Evacuation Routes

Primary evacuation of the facility will be through the Main Gate (<insert name> Road). Normal procedures for the accounting and searching of personnel and vehicles that exit the facility will be implemented unless otherwise directed by the FSO or Designated Authorities of the Contracting Government.

If there is cause for the primary evacuation route to become unserviceable, the secondary exit point from the facility is at the <insert name> Road gate. Normal procedures for the accounting and searching of personnel and vehicles that exit the facility will be implemented unless otherwise directed by the FSO or Designated Authorities of the Contracting Government.

If both the primary and secondary exits/egress points from the facility are unserviceable, facility personnel and visitors are instructed to follow the orders of the FSO, the next person in command, or Designated Authorities.

***ANNEX 1***

***APPROVAL LETTER OF  
HARBOR POINT FACILITY SECURITY PLAN***

***CONTRACTING GOVERNMENT'S STATEMENT OF COMPLIANCE***

**Form of a Statement of Compliance of a Facility**

**STATEMENT OF COMPLIANCE OF PORT FACILITY**

*(Official seal) (State)*

Statement Number

**Issued under the provisions of Part B of the  
INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT  
FACILITIES (ISPS CODE)**

The Government of \_\_\_\_\_  
*(name of the State)*

Name of the Facility : .....

Address of the Facility : .....

THIS IS TO CERTIFY that the compliance of this port facility with the provisions of chapter XI-2 and part A of the International Code for the Security of Ships and of Port Facilities (ISPS Code) has been verified and that this port facility operates in accordance with the approved Facility Security Plan. This plan has been approved for the following *<specify the types of operations, types of ship or activities or other relevant information> (delete as appropriate):*

Passenger ship

Passenger high speed craft

Cargo high speed craft

Bulk carrier

Oil tanker

Chemical tanker

Gas carrier

Mobile offshore Drilling Units

Cargo ships other than those referred to above

This Statement of Compliance is valid until ....., subject to verifications (as indicated overleaf)

Issued at.....  
*(place of issue of the certificate)*

Date of issue .....  
*(signature of the duly authorized official issuing the Certificate)*

*(Seal or stamp of issuing authority, as appropriate)*

## ENDORSEMENT FOR VERIFICATIONS

The Government of *<insert name of the State>* has established that the validity of this Document of Compliance is subject to *<insert relevant details of the verifications (e.g., mandatory annual or unscheduled)>*.

THIS IS TO CERTIFY that, during a verification carried out in accordance with paragraph B/16.40.3 of the ISPS Code, the *<insert port facility name>* was found to comply with the relevant provisions of chapter XI-2 of the SOLAS 74 Convention and Part A of the ISPS Code.

1<sup>st</sup> VERIFICATION

Signed.....  
*(Signature of authorized official)*

Place .....

Date .....

2<sup>nd</sup> VERIFICATION

Signed.....  
*(Signature of authorized official)*

Place .....

Date .....

3<sup>rd</sup> VERIFICATION

Signed.....  
*(Signature of authorized official)*

Place .....

Date .....

4<sup>th</sup> VERIFICATION

Signed.....  
*(Signature of authorized official)*

Place .....

Date .....

***ANNEX 2***

***EMERGENCY SERVICES AND KEY CONTACT TELEPHONE  
NUMBERS LIST***

<b>KEY CONTACT TELEPHONE NUMBERS</b>	
	Phone No.
1	Facility Security Officer
2	Contracting Government Maritime Security Department
3	National Response Center <span style="float: right;">1 800 424 8802</span>
4	Security Network Communications Numbers
5	Gate Security
6	Harbor Master/Port Captain
7	Local Police
8	Local Fire Department
9	Coast Guard
10	Emergency Medical/Ambulance Service
11	Local Police
12	State/Federal Law Enforcement/Intelligence Unit
13	Bomb Squad. (Explosive Ordinance Disposal [EOD] Team)
14	Service Vessels – Pilots
15	Service Vessels – Tugs
16	Service Vessels – Fuel/oil bunkering
17	Service Vessels – Potable water
18	Service Vessels – Waste transfer/transport
19	Other

*ANNEX 3*

*DECLARATION OF SECURITY*

**(To be issued when deemed necessary by the Contracting Government or the incoming ship [or its Flag Administration] and approved [signed] by both the Facility Security Officer and the Ship Master or Ship Security Officer)**

## DECLARATION of SECURITY

Name of Ship:	
Port of Registry	
IMO Number	
Name of Facility	

This Declaration of Security is valid from ..... until ....., for the following activities

.....

*(list the activities with relevant details)*

under the following security levels

Security level(s) for the ship:	
Security level(s) for the port facility	

The port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of Part A of the International Code for the Security of Ships and of Port Facilities.

	The affixing of the initials of the SSO or FSO under these columns indicates that the activity will be done, in accordance with relevant approved plan, by	
Activity	The port facility:	The ship:
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access		
Controlling access to the port facility		
Controlling access to the ship		
Monitoring of the ship, including berthing areas and areas surrounding the ship		
Handling the cargo		
Delivery of ship's stores		
Handling unaccompanied baggage		
Controlling the embarkation of persons and their effects		
Ensuring that security communication is readily available between the ship and port facility		

The signatories to this agreement certify that security measures and arrangements for both the port facility and the ship during the specified activities meet the provisions of chapter XI-2 and Part A of Code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

Dated at .....on the .....

## DECLARATION of SECURITY

Signed for and on behalf of	
the port facility:	the ship:
<i>(Signature of Facility Security Officer)</i>	<i>(Signature of Master or Ship Security Officer)</i>

Name and title of person who signed	
Name:	Name:
Title:	Title:

<b>Contact Details</b> <i>(to be completed as appropriate)</i> <i>(indicate the telephone numbers or the radio channels or frequencies to be used)</i>	
for the port facility:	for the ship:

Facility:  
Facility Security Officer:

Master:  
Ship Security Officer:  
Company:  
Company Security Officer:

***ANNEX 4***  
***PERSONNEL/VISITOR LOG SHEET***



*ANNEX 5*

*TELEPHONIC BOMB/THREAT REGISTER FORM*

## **TELEPHONIC BOMB/THREAT REGISTER FORM**

### **IF BOMB THREAT IS RECEIVED, ASK THE CALLER....**

WHEN IS THE BOMB TO GO OFF?

WHERE IS THE BOMB TO GO OFF?

WHAT KIND OF BOMB IS IT?

WHAT DOES THE BOMB LOOK LIKE?

WHERE ARE YOU CALLING FROM?

### **TELEPHONE CALL RECEIVED ON**

a. Phone Number (include area code)

b. Location

### **DETAILS OF CALL**

a. Date

b. Day of Week

c. Time

### **CONTEXT OF CONVERSATION**

**BACKGROUND NOISES** (Describe street sounds, voices, music, etc. If more space is needed, continue on reverse or additional sheet.)

### **INFORMATION ABOUT CALLER/VOICE CHARACTERISTICS**

a. Sex

b. Age

- c. Accent
- d. Educational Level
- e. Attitude (Calm, Nervous, Serious)
- f. Political, national, activist/terror group affiliation
- g. Other identifying characteristics

**WITNESSES TO THE CALL**

- a. Yes/No
- b. Name and location, telephone

**DO YOU HAVE ANY SUSPICION AS TO THE IDENTITY OF THE CALLER?**

- a. No
- b. Yes (List Name/s)

**YOUR NAME and DUTY POSITION:**

**ADDITIONAL NOTES**

**ANNEX 6**

**FACILITY SECURITY PLAN AND  
USCG REGULATION CROSS REFERENCE**

*{Note: After the FSP is complete, the attached cross reference table should be filled out to serve as a simple audit of the Plan and to satisfy U.S. Coast Guard regulation 33 CFR Subpart 105.405(a), which requires such an index.}*

**Cross Reference from USCG Maritime Facility Security Regulation (33 CFR Part 105) to Facility Security Plan**

<b>Part 105</b>	<b>Topic</b>	<b>Facility Security Plan Section</b>
<b>Subpart A</b>	<b>General</b>	
105.100	Definitions	
105.105	Applicability	
105.106	Public access areas	
105.110	Exemptions	
105.115	Compliance dates	
105.120	Compliance documentation	
105.125	Noncompliance	
105.130	Waivers	
105.135	Equivalents	
105.140	Alternative Security Program	
105.145	Maritime Security (MARSEC) Directive	
105.150	Right to appeal	
<b>Subpart B</b>	<b>Facility Security Requirements</b>	
105.200	Owner or operator	
105.205	Facility Security Officer (FSO)	
105.210	Facility personnel with security duties	
105.215	Security training for all other facility personnel	
105.220	Drill and exercise requirements	
105.225	Facility recordkeeping requirements	
105.230	Maritime Security (MARSEC) Level coordination and implementation	
105.235	Communications	
105.240	Procedures for interfacing with vessels	
105.245	Declaration of Security (DoS)	
105.250	Security systems and equipment maintenance	
105.255	Security measures for access control	
105.260	Security measures for restricted areas	
105.265	Security measures for handling cargo	
105.270	Security measures for delivery of vessel stores and bunkers	
105.275	Security measures for monitoring	

<b>Part 105</b>	<b>Topic</b>	<b>Facility Security Plan Section</b>
105.280	Security incident procedures	
105.285	Additional requirements – passengers and ferry facilities	
105.290	Additional requirements – cruise ship terminals	
105.295	Additional requirements – Certain Dangerous Cargo (CDC) facilities	
105.296	Additional requirements – barge fleeting facilities	
<b>Subpart C</b>	<b>Facility Security Assessment (FSA)</b>	
105.300	General	
105.305	FSA requirements	
105.310	Submission requirements	
<b>Subpart D</b>	<b>Facility Security Plan (FSP)</b>	
105.400	General	
105.405	Format and content of the FSP	
105.410	Submission and approval	
105.415	Amendment and audit	