



**ISPS (Parts A and B)
International Ship and Port Facility Security Code
International Maritime Organization**

Facility Security Assessments

- Must be carried out by:
 1. The Contracting Government (as party to the 1974 SOLAS Convention or, 1988 SOLAS Protocol)
 2. A Designated Authority (within the government, and as identified by the Contracting Government per section 4.2 of Part B)
 3. A “recognized security organization” (must be authorized by the Contracting Government based on the RSO’s ability to demonstrate proficiency in 13 specific areas as listed in section 15.4 of Part B. A port facility operator may be authorized as an RSO as per section 4.7 of Part B)

- Must be approved by:
 1. The Contracting Government
 2. A Designated Authority

- Must be “periodically” reviewed and updated when threats change or when changes are made to the port facility that affects its security.

- Must include at least the following (section 15.5 of Part A):
 1. Identification and evaluation of assets and infrastructure that must be protected (at least the 9 items listed in section 15.7 of Part B)
 2. Identification of possible threats to assets and infrastructure (at least the 9 threats listed in section 15.11 of Part B) and the likelihood of their occurrence, in order to prioritize security measures
 3. Identification, selection and prioritization of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability
 4. Identification of vulnerabilities and weaknesses, including human factors, in the infrastructure, policies and procedures. (at least the 12 items listed in section 15.16 of Part B)



- Must address the following (section 15.3 of Part B):
 1. Physical security
 2. Structural integrity
 3. Personnel protection systems
 4. Procedural policies
 5. Communication systems including radio, telephone and computer networks
 6. Relevant transportation infrastructure
 7. Utilities
 8. Other areas or adjacent structures that may, if damaged, or used for illicit observation, pose a risk to persons, property , or operations within the port facility

- Must include an overall assessment of risk, based on information from relevant national security organizations regarding the following (section 15.10 of Part B):
 1. Particular aspects of the facility that make it a likely target
 2. Likely consequences of an attack
 3. Capability and intent of potential attackers
 4. Possible types of attack
 5. May cover more than one facility if the operator, location, operation, equipment and design are similar, contingent on the contracting government's approval.
 6. A post-assessment report is required consisting of the following:
 - a. How the assessment was conducted
 - b. Description of vulnerabilities, and the possible countermeasures that could be employed for each.

Facility Security Plans

- Must be based on the Facility Security Assessment
- Must make provisions for the three security levels as defined by IMO
- Must take into account the guidance given in Part B of the ISPS
- Must be in the working language of the port facility
- Must be created by:
 1. The FSO
 2. A “recognized security organization”

- Must be approved by:
 1. The Contracting Government



2. A Designated Authority

- Must include, at least, the following (section 16.3 of Part A):
 1. Measures designed to prevent weapons etc. from being introduced into the port facility or on board a ship
 2. Measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restricted areas of the facility;
 3. Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface
 4. Procedures for responding to any security instructions the contracting government, in whose territory the port facility is located, may give at security level 3
 5. Procedures for evacuation in case of security threats or breaches of security
 6. Duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects
 7. Procedures for interfacing with ship security activities
 8. Procedures for the regular review audit and amendment of the plan
 9. Procedures for reporting security incidents
 10. Identification of the port facility security officer including 24-hour contact details
 11. Measures to ensure the security of the information contained in the plan
 12. Measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility
 13. Procedures for auditing the port facility security plan
 14. Procedures for responding in case the ship security alert system of a ship at the port facility has been activated
 15. Procedures for facilitating shore leave for ship's personnel or personnel changes, as well as the access and identification of visitors to the ship including representatives of seafarers' welfare and labor organizations.
 16. **Additional requirements per section 16.3-16.8 of Part B follow below
 17. Description of the facility's security organization and its role and the duties, responsibilities and training requirements of its personnel
 18. Description of links and communications systems with relevant authorities, neighboring facilities and ships in port
 19. Description of security measures for each of levels 1-3 (as detailed in sections 16.9-16.54 of Part B)



20. Description of reporting procedures to the appropriate Contracting Government's contact points
21. Provisions for the retention of records of incidents, threats, reviews, audits, training drills and exercises
22. Implementation schedule for security measures not yet in place and a description of approved temporary measures to cover interim period if not in place in a "reasonable period"
23. Procedures related to cargo handling, ship stores and the documentation of hazardous cargo including their location within the facility
24. Measures to ensure continuous operation of all safety features, procedures, equipment and communications systems
25. Means of alerting waterside patrols including bomb searches and underwater searches

Training, Drills and Exercises

- FSO and appropriate facility security personnel must receive training in at least the 20 items listed in section 18.1 of Part B as appropriate per location
- Personnel that are assigned duties in the plan must be trained and able to perform the duties as assigned. Training areas are listed in 18.2 of Part B
- All remaining facility personnel are required to receive training on the relevant provisions of the FSP including (section 18.3 of Part B):
 1. Meaning and consequential requirements for each security level
 2. Recognition of weapons etc.
 3. Recognition of persons who may threaten security
 4. Awareness of techniques used to circumvent security measures
- The training method and format is not specified in either Part A or B and presume e-learning or similar will be acceptable
- Drills must be carried out every three months (18.5 Part B) unless specified otherwise. The drills should test individual elements of the plan including the threats listed in section 15.11 Part B
- FSO must participate in exercises at appropriate intervals (18.6 Part B)
 1. Once per year and not more than 18 months between exercises



2. Should include relevant authorities within the Contracting Government, CSO's and SSO's
3. Exercises should test communications coordination, and resource availability and response
4. May be full-scale/live or tabletop simulation
5. May be combined with other exercises including port State authority exercises

Additional Notes and Requirements

Functional Requirements for Code Compliance (section 1.3)

1. Threat assessment
 2. Establishment/maintenance of communication protocols
 3. Prevention of unauthorized access to secure areas
 4. Prevention of the introduction of unauthorized weapons etc to secure areas.
 5. Provision of means for raising the alarm in response to a threat or incident
 6. Establishment/maintenance of a security plan
 7. Training, drills and exercises to ensure familiarity with plans and procedures
- The CSO for a vessel operating company is responsible for ensuring that the security assessments are carried out, security plans are developed and submitted for approval, and thereafter implemented and maintained, and for liaison with SSO's and FSO's. (Note that no requirement is listed for Terminal Operating Companies to designate a CSO. Section 11.2 in Part A details thirteen responsibilities of a CSO specifically for a company that operates ships...no similar description exists in the port facility section of the code. Again in section 1.9 of Part B the CSO requirement is restated for ship operating companies only.)
 - An FSO is required (per section 17.2 of Part A and section 1.18 of Part B) and is responsible for the following:
 1. Conducting an initial comprehensive security survey of the port facility taking into account the relevant port facility security assessment
 2. Ensuring the development and maintenance of the port facility security plan
 3. Implementing and exercising the port 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 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
 6. Enhancing security awareness and vigilance of the port facility personnel
 7. Ensuring adequate training has been provided to personnel responsible for the security of the port facility
 8. Reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility
 9. Coordinating implementation of the port facility security plan with the appropriate company and ship security officer(s)
 10. Coordinating with security services, as appropriate
 11. Ensuring that standards for personnel responsible for security of the port facility are met
 12. Ensuring that security equipment is properly operated, tested, calibrated and maintained, if any
 13. Assisting ship security officers in confirming the identity of those seeking to board the ship when requested.
- Contracting governments are responsible for, and may not delegate the following:
 1. Setting the appropriate security levels
 2. Establishing the requirements for the Declaration of Security
 3. Approving assessments and plans, as well as any subsequent amendments
 4. Exercising control and compliance measures
 5. Designating which facilities are required to designate an FSO and prepare a FSP
 - Contracting Governments may delegate the following duties to “a recognized security organization”:
 1. Conducting Facility Security Assessments (approval of the assessment and any subsequent amendments remains the responsibility of the contracting government)
 2. Preparing Facility Security Plans (approval of plans and subsequent amendments remains the responsibility of the contracting government)
 - Declaration Of Security (DOS) is generally required when:
 1. Ship and port are not on same security level (section 7.7 of Part A) (Per section 4.11 of Part B, the CSO or SSO should “liaise at the earliest opportunity” with the FSO. The Contracting Government is responsible for establishing procedures for



- communications between FSO's and SSO's per section 4.25 of Part B) If the ship is at a higher security level than the port facility then the CSO or SSO is responsible (per section 4.12 of Part B) for informing the FSO who then "shall report the matter to the competent authority" (is this intended to be the Contracting Government / Recognized Security Organization, or the CSO?) and liaise with the SSO to "coordinate appropriate actions"
2. Port authority has made it an SOP for each ship/port interface
 3. There has been a threat or incident
 4. Either ship or port is not required to have an approved plan
- The DOS must be completed in English, Spanish or French or, in a language that is common to both port and ship per section 5.5 of Part B
 - A sample DOS is provided in appendix 1 of Part B
 - A sample Statement of Compliance of a Port Facility is provided in appendix 2 of Part B
 - Personnel conducting internal audits must be independent of the activities being audited
 - The plan may cover more than one facility if the operator, location, operation, equipment and design are similar based on the contracting governments approval.
 - Part A of the ISPS is considered mandatory. Section 16.3 of Part A requires that the FSP "shall be developed taking into account the guidance given in part B of the code" which, presume this does not mean that the following elements (among others in Part B) represent firm requirements:
 1. Section 16.19.6 of Part B refers to port facilities providing patrol vessels to enhance water-side security at level 2
 2. Sections 16.30-16.34 of Part B refers port facilities performing seal checking and actual contents checking while at level 1
 3. Section 16.38 of Part B refers to port facilities checking ship stores, searching the delivery vehicle and requiring advanced notification of composition of load, driver details and vehicle registration at level 1
 4. Section 16.45 of Part B refers to port facilities checking/screening unaccompanied baggage prior to receipt at the facility at level 1



5. Section 16.49 of Part B refers to the port facility security organization having the capability to monitor the entire facility, the ships alongside and surrounding areas, and all nearby approaches, on land and water, at all times including night hours and periods of limited visibility.

NVIC (No. 11-02)
Navigation and Vessel Inspection Circular
United States Coast Guard

Facility Security Assessments (section 1.8)

- Per MTSA 2002, the company itself can conduct the assessment. NVIC 11-02 supports this and adds that the FSO may delegate the task to “a person(s) with skills to evaluate the security of a facility” Should be done in cooperation with the COTP (US Coast Guard Captain of the Port), local Port Security Committees and Harbor Safety Committees per section 2 (b)
- Must include an analysis of possible threats and vulnerabilities of the facility as per the following:
 1. a list of specific threat scenarios for each element in a facility (intrusion and attack on power supply)
 2. an assignment of consequence level to the facility as a whole (LNG terminal or bulk grain loader etc)
 3. a vulnerability assessment of each element in the facility including its security personnel and procedures as well as its physical layout/location/construction etc.
 4. a list of mitigation strategies for each relevant threat scenario (relevance is determined as a score based on matrix of consequence level and vulnerability assessment)
 5. implementation methods, (efforts are to be focused on reducing vulnerabilities, given that consequence levels and threat scenarios are not controllable variables)
- Must include a detailed examination of existing protective measures, procedures and operations as per the following:
 1. The general layout of the facility;
 2. The location and function of each actual or potential access point to the facility;



3. Existing protective measures including inspection, control and monitoring equipment, personnel identification documents and communication, alarms, lighting, access control, and similar systems.
4. Numerical strength, reliability, and security duties of the facility's personnel;
5. Security doors, barriers, and lighting.
6. The location of areas which should have restricted access, such as control stations, communications centers, cargo storage areas, etc.;
7. The emergency and stand-by equipment available to maintain essential services;
8. Response procedures for fire or other emergency conditions;
9. Existing security and safety equipment for protection of personnel and visitors;
10. The level of supervision of the facility's crew, vendors, repair technicians, dock workers, etc.;
11. Existing agreements with private security companies providing facility security services at all MARSEC levels, including any security forces contracted by visiting vessels;
12. Procedures for control of security keys and other access prevention systems;
13. Cargo and vessel stores operations; and
14. Response capability to incidents.

Facility Security Plans (section 1.9)

- Must include, at least the following:
 1. Measures and/or equipment designed to prevent or deter the unauthorized carriage of weapons, dangerous substances, and devices intended for use against people, vessels, or ports.
 2. Identification of the restricted areas and measures and/or equipment for the prevention of unauthorized access to the facility and to restricted areas of the facility;
 3. Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the facility or the vessel/port interface;
 4. Procedures for evacuation in case of security threats or breaches of security;
 5. Duties of facility personnel assigned security responsibilities and of other facility personnel on security aspects;
 6. Procedures for auditing the security activities, procedures for training, exercises, and drills associated with the plan;
 7. Procedures for interfacing with port and vessel security activities;
 8. Procedures for the periodic review and updating of the plan;



9. Procedures for reporting transportation security incidents;
10. Procedures for summoning emergency, safety, or security personnel including: local fire and police departments, SWAT, bomb disposal units, divers, hospital and EMT services, etc.;
11. Identification of the Facility Security Officer including 24-hour contact details;
12. Measures to ensure the security of the information contained in the plan;
13. Measures designed to ensure effective security of cargo and the cargo handling equipment at the facility.
14. Procedures for auditing the facility plan;
15. Procedures for responding in case the ship security alert system of a ship at the facility has been activated; and
16. 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.

Training Drills and Exercises

- Drills should be conducted every three months
- Exercises should be conducted every 12 months
- Communication and notification procedures should be included in drills and exercises
- Training should include the following items:
 1. Security administration;
 2. Relevant national and international conventions, codes, and recommendations;
 3. Relevant government legislation and regulations;
 4. Responsibilities and functions of other involved organizations;
 5. Risk, threat, and vulnerability assessments;
 6. Security assessments and inspections;
 7. Ship and port operations and conditions;
 8. Vessel and *facility* security measures;
 9. Emergency preparedness, response and contingency planning;
 10. Instruction techniques for security training and education, including measures and procedures;
 11. Handling sensitive security related information and communications
 12. Knowledge of current security threats and patterns;



13. Recognition and detection of weapons, dangerous substances, and devices;
14. Recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to commit *transportation security incidents*;
15. Techniques used to circumvent security measures;
16. Security devices and systems, and their operational limitations;
17. Methods of conducting audits, inspections, control, and monitoring;
18. Methods of physical searches and non-intrusive inspections;
19. Security drills and exercises, including drills and exercise with ships; and
20. Assessment of security drills and exercises.

Additional Notes and Requirements

- Records of the following should be kept for at least two years (section 1.11):
 1. Training, drills, and exercises;
 2. Reports of transportation security incidents;
 3. Report of breaches of security;
 4. Changes in MARSEC levels;
 5. Maintenance, calibration, and testing of security equipment;
 6. Communications relating to the direct security of the facility such as specific threats to the facility;
 7. Periodic review of the security assessment.
- NVIC 11-02 is a “benchmark” until final regulations are published
- USCG will develop a new set of regulations to implement the requirements of the MTSA and ISPS (new draft regulations due in June)
- Declaration of Security (DOS) should be completed between VSO's and FSO's at MARSEC 1 or vessels carrying (CDC) Certain Dangerous Cargo (as defined in section 1.2). DOS is required for all vessels when at MARSEC 2 and 3.
- MARSEC 1, 2 and 3 are used to communicate threat levels which, relate to HSAS levels (Homeland Security Advisory System) as follows:
 1. MARSEC 1 = HSAS 1-3 (green, blue, yellow)
 2. MARSEC 2 = HSAS 4 (orange)
 3. MARSEC 3 = HSAS 5 (red)



- FSO is required per section 1.7 of Enclosure (1). One FSO may cover several facilities. An FSO may have other unrelated duties in addition security responsibilities as long as the person remains capable as FSO. Duties include:
 1. Conducting an initial comprehensive security assessment of the facility in order to prepare a Facility Security Plan;
 2. Implementing and exercising the Facility Security Plan;
 3. Undertaking regular security inspections of the facility to ensure the continuation of appropriate security measures;
 4. 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 facility;
 5. Enhancing security awareness and vigilance;
 6. Ensuring adequate training for personnel responsible for security of the facility;
 7. Reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the facility;
 8. Coordinating implementation of the Facility Security Plan with the master(s) or Vessel Security Officer(s) as appropriate;
 9. Coordinating with security services, as appropriate;
 10. Ensuring that standards for personnel responsible for security of the facility are met;
 11. Arranging for a timely response by law enforcement personnel, and others, to any incident.

- Following implementation guidelines are based on existing NVIC's and the ISPS:
 1. Enclosure (1) information for developing a comprehensive security program.
 2. Enclosure (2) detailed measures to be incorporated into a facility security plan
 3. Enclosure (3) is a comprehensive sample audit checklist
 4. Enclosure (4) is a sample Declaration of Security.
 5. Enclosure (5) a simplified risk based security assessment tool

MTSA 2002

United States Maritime Transportation Security Act

Facility Security Assessments

- Assessment can be conducted by the facility owner or operator



- Must be updated every five years

- Must cover the following:
 1. Identification and evaluation of critical assets and infrastructures
 2. Identification of the threats to those assets and infrastructures
 3. Identification of weaknesses in:
 - physical security
 - cargo security
 - structural integrity
 - protection systems
 - procedural policies
 - communications systems
 - transportation infrastructure
 - utilities
 - contingency response

Facility Security Plans

- Deadline is six months after the Secretary prescribes interim final regulations (expected spring 2003?)

- Must be updated every five years

- Must be resubmitted for approval for each change to the facility that may substantially affect security

- Must cover the following:
 1. Facility Security Officer
 2. Physical security, cargo security, and personnel security
 3. Secure access to areas of the vessel or facility
 4. Procedural security policies, communications systems, and other security systems.
 5. Deterrence and response measures and responsible authorities
 6. Security training including periodic unannounced drills

Transportation security cards



- Required for unescorted access to secure areas and/or information
- Must include biometrics (realistic?)

Grants

- The project must be consistent with Coast Guard vulnerability assessments and be in compliance with area regulations. Funding is provided for the following purposes:
 1. Salary, benefits, overtime compensation, retirement contributions, and other costs of additional Coast Guard mandated security personnel.
 2. The cost of acquisition, operation, and maintenance of security equipment or facilities to be used for security monitoring and recording remote surveillance, concealed video systems.
 3. Security gates and fencing and marine barriers for designated security zones
 4. Security-related lighting systems.
 5. Security vessels, and other security-related infrastructure or equipment that contributes to the overall security of personnel or cargo.
 6. The cost of screening equipment, including equipment that detects weapons of mass destruction and conventional explosives, and of testing and evaluating such equipment, to certify secure systems of transportation.
 7. The cost of conducting vulnerability assessments to evaluate and make recommendations with respect to security.
- Federal funding can't exceed 75 percent of the total cost of the project unless:
 1. The project's total cost is below \$25,000
 2. The Secretary of Transportation determines that a proposed project merits support and cannot be undertaken without a higher rate of Federal support
- The Secretary of Transportation shall ensure co-operation among relevant community members and that there is no duplication of funding.