Asia-Pacific
Economic Cooperation

2005/STAR/012
Maritime Security Panel 1

International Port Security Program

Submitted by: U.S.A

Third Conference on Secure Trade in the APEC Region
Incheon, Korea
25-26 February 2005

International Port Security Program

Implementation of the IMO International Ship and Port Facility Security (ISPS) Code and US Maritime Transportation and Security Act (MTSA)

CDR Joseph LoSciuto
U. S. Coast Guard Headquarters
Port Security Directorate
Chief, International Port Security Program
(202) 366-1497
Jlosciuto@msc.uscg.mil

United States Approach to the ISPS Code

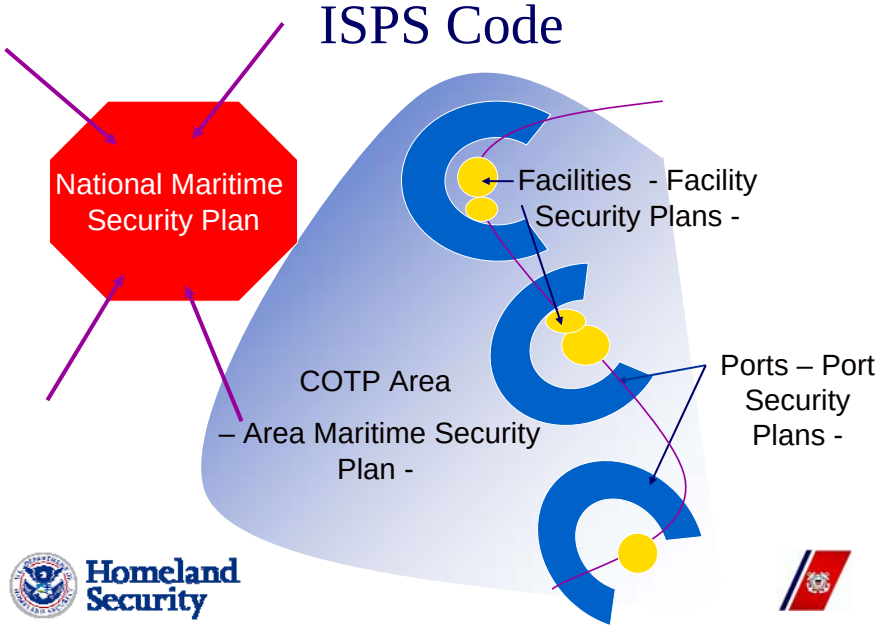
- Port area is the port facility
- Coast Guard Captain of the Port is the Port Facility Security Officer
- Assessment is conducted by port area stakeholders
- Additional requirements for individual terminals (layered approach)
- ISPS requirements extended to domestic facilities
- Security directives

Other Issues Related to Port Security

- Improving maritime domain awareness:
  - Automated Identification Systems
  - Long-range tracking of ships
- Coastal watch programs
- Seafarer and maritime worker identification credentials
- Ship security alert system
- Continuous Synopsis Record

Homeland Security

United States Approach to the ISPS Code



Homeland Security

U. S. Policy Technical Assistance

- USCG Navigation Vessel Inspection Circulars (NVICs)

- NVIC 9-02, Change (1) - Port Security Plans
- NVIC 04-03 - Vessel Security Plans
- NVIC 03-03 - Facility Security Plans
- NVIC 05-03 - OCS Facility Plans
- Web site:http://www.uscg.mil/hq/g-m/nvic/index00.htm

Coast Guard ISPS/MTSA "HELP Desk"
Web site: http://www.uscg.mil/hq/g-m/mp/ipsp.shtml

E-mail: fldr-g-moc-@comdt.uscg.mil

Homeland Security

International Port Security Program

- **Asia-Pacific Region, CDR Jung Lawrence (Japan)**
  Phone: 011 81-425-52-2511 Ext. 58405 E-mail: jlawrence@d14.uscg.mil
- **Europe/Mid-East Region, LCDR Brian Gilda (Netherlands)**
  Phone: +31 10-442-4458 E-Mail: Bgilda@acteur.uscg.mil
- **South/Central America (East) Mr. Peyton Coleman**
  Phone: (757) 398-6786 E-Mail: pcoleman@lantd5.uscg.mil
- **South/Central America (West) Mr. Steve Danscuk**
  Phone: (510) 437-5839 E-Mail: sdanscuk@d11.uscg.mil

Homeland Security


U.S. DEPARTMENT OF HOMELAND SECURITY
Homeland
Security

Implementation Process

Who is the Designated Authority? (SOLAS regulation XI-2/1.11)

The United States Coast Guard (USCG), as the lead national agency for maritime homeland security, is the Designated Authority.

What is the national legislative basis for the implementation of the ISPS Code? (SOLAS regulations XI-2/2 and XI-2/10)

The United States Government enacted the Maritime Transportation Security Act (MTSA) on November 25, 2002. This legislation required the Secretary of Homeland Security to implement regulations that provide for comprehensive maritime security. The vast majority of the Secretary's maritime security authorities and responsibilities were delegated to the Commandant of the United States Coast Guard.

The Coast Guard developed regulations to carry out the intent of the provisions of the MTSA that reflected the requirements of the International Ship and Port Security (ISPS) Code. These regulations were published as five parts to the Code of Federal Regulations (CFR). The five parts are:

- Part 101 – Maritime Security: General,
- Part 103 – Maritime Security: Area (Port) Maritime Security,
- Part 104 – Maritime Security: Vessels,
- Part 105 – Maritime Security: Facilities
- Part 106 – Maritime Security: Outer Continental Shelf (OCS) Facilities.

The deadline for all required compliance with the MTSA regulations was the same as the deadline for ISPS Code implementation, July 1, 2004.

What guidance to industry was released to implement the ISPS Code? (SOLAS regulations XI-2/2 and XI-2/10)

In addition to the MTSA regulations published in the CFR, a series of USCG Navigation and Vessel Inspection Circulars were also released. A Navigation and Vessel Inspection Circular (NVIC) provides detailed guidance about the enforcement or compliance with certain Federal marine safety regulations and Coast Guard marine safety and security programs. While NVIC's are non-directive, meaning that they do not have the force of law, they are important "tools" for complying with the law. The NVICs related to MTSA/ISPS Code enforcement included:

- NVIC 09-02 Development of Area Maritime Security Committees and Area Maritime Security Plans for U.S. Ports
- NVIC 03-03 Implementation of MTSA Regulations for Facilities
- NVIC 04-03 Verification of Vessel Security Plans for domestic vessels in accordance with MTSA Regulations and ISPS Code

- NVIC 05-03 Implementation of MTSA Regulations for Outer Continental Shelf Facilities
- NVIC 06-03 Port State Control Targeting and Boarding Policy for Vessel Security and Safety
- NVIC 06-04 Voluntary screening for owners or operators
- NVIC 10-04 Guidelines For Handling Of Sensitive Security Information (SSI)
- NVIC 11-02 Recommended Security Guidelines for Facilities
- NVIC 10-02 Security Guidelines for Vessels

These NVICs can also be found at the following web address: http://www.uscg.mil/hq/g-m/mp/mtsa.shtml.

The Coast Guard engaged in a wide-ranging public outreach effort to inform maritime industry and other port stakeholders of the MTSA regulations and the ISPS Code. This effort included media briefings, informational brochures, and press releases, public meetings held in each Coast Guard Captain of the Port (COTP) zone, and meetings held under the auspices of each designated Area Maritime Security Committee whose membership includes representatives of the maritime transportation industry. Each Coast Guard COTP engaged in individual direct outreach within their port as they serve as the ISPS Code defined Port Facility Security Officer (PFSO)/Federal Maritime Security Coordinator. Finally, the Coast Guard established an MTSA-ISPS Help Desk that included an Internet website and toll-free telephone line.

What are the means of communication with port facilities regarding ISPS Code implementation? (SOLAS regulations XI-2/3 and XI-2/10)

As discussed above, the Coast Guard published interim and final rules detailing the MTSA regulations that implemented ISPS Code requirements, in addition to other public outreach that occurred on the local level. The USCG determined that approximately 3100 facilities are required to comply with the MSTA regulations. Each Coast Guard COTP acting as the PFSO is responsible for direct communication to all entities within his or her port as it relates to Code implementation and the verification thereof.

What processes are in place to document initial and subsequent compliance with the ISPS Code? (SOLAS regulation XI-2/10.2)

An initial review by each COTP was conducted to identify each vessel owner and facility within their Area of Operation (AOR) that would be affected by ISPS and MTSA. The vessel and facility's information was then entered into a USCG national database, which documented when a security plan was submitted, when it was reviewed, when USCG personnel conducted an initial verification inspection. The database is searchable for FSP approval dates and scheduling annual COTP verification inspections. In addition, facility owners and operators are required to perform annual audits of their FSP to reflect their current operations and validated that vulnerabilities identified in their last assessment have not changed.

What is the Contracting Government's definition for a Port Facility? (SOLAS regulation XI-2/1.1)

For purposes of implementing the ISPS Code, the United States designated each Coast Guard Captain of the Port's AOR as a port facility. Under MTSA regulations, operations within the port facility that were required to meet the ISPS Code included:

The MTSA regulations further expanded domestic security requirements defining operations within the port as a "facility" if it included:

(1) Handles class 1 (explosive) materials or other dangerous cargoes within or contiguous to waterfront facilities. (as defined in 33 CFR part 126)
(2) Handles liquefied natural gas and liquefied hazardous gas (as defined in 33CFR127)
(3) Transfers oil or hazardous material in bulk (as defined in 33 CFR part 154)
(4) Receives vessels certificated to carry more than 150 passengers, except those vessels not carrying and not embarking or disembarking passengers at the facility
(5) Receives vessels subject to the International Convention for Safety of Life at Sea (SOLAS), 1974, Chapter XI
(6) Receives foreign cargo vessels greater than 100 gross register tons
(7) Receives U.S. cargo vessels, greater than 100 gross register tons that are:
    - Ocean or unlimited coastwise vessels on inland and Great Lakes routes.
    - Vessels on an international voyage.
    - Offshore supply vessels
    - Seagoing barges
    - Flammable and combustible liquid cargo in bulk.
(8) Barge fleeting facilities that receive barges carrying in bulk regulated cargoes or Certain Dangerous Cargoes.

Under MTSA, the United States Coast Guard was responsible for approving approximately 3100 facility security plans.

What are the procedures used to determine the extent to which port facilities are required to comply with the ISPS Code, with particular reference to those port facilities that occasionally serve ships on international voyages? (SOLAS regulations XI-2/1, XI-2/2.2)

All port facilities serving vessels over 100 gross tons, carry more than 6 passengers for hire or subject to the International Convention for Safety of Life at Sea (SOLAS), 1974, Chapter XI that are occasionally engaged in international voyages were required to comply fully with the ISPS Code. To address the varying levels of risk during periods of intermittent operations at facilities, FSP must include the security measures that a facility will implement when not receiving MTSA regulated vessels or storing cargo intended for MTSA regulated vessels as well as the security measures it will implement prior to resuming regulated operations.

Has the Contracting Government concluded in writing bi-lateral or multi-lateral agreements with other Contracting Governments on alternative security agreements? (SOLAS regulation XI-2/11.1)

Yes, currently the USCG has established a bi-lateral agreement with Canada and the United Kingdom.

Has the Contracting Government allowed a port facility or group of port facilities to implement equivalent security arrangements? (SOLAS XI-2/12.1)

No equivalent security arrangements have been approved. The MTSA security requirements are performance based providing the owner or operator with the latitude to determine what security measures best meets their needs based on their specific operation, location, or etc.

Who has the responsibility for notifying and updating the IMO with information in accordance with SOLAS regulation XI-2/13? (SOLAS regulation XI-2/13)

Rear Admiral Larry Hereth, Director of Port Security, USCG, Washington, D.C.

Port Facility Security Assessment (PFSA)

Who conducts PFSAs? (SOLAS regulation XI-2/10.2.1, ISPS code section A/15.2 and 15.2.1)

Each Coast Guard Captain of the Port, acting as the PFSO, was responsible for conducting a PFSA for his/her port facility.

Each individual facility within the port facility to which MTSA was applicable was required to designate a company security officer (CSO) and a facility security officer (FSO), to conduct a facility security assessment, and implement a facility security plan.

Third parties could be used in any aspect of the individual facility PFSA if they had the appropriate skills and if the Facility Security Officer (FSO) reviewed and accepted their work.

How are PFSA's conducted and approved? (ISPS Code section A/15.2 and 15.2.1)

Each Coast Guard, Captain of the Port, acting as the PFSO conducted a PFSA for his/her port facility under the guidance set by Commandant, U. S. Coast Guard, to insure a national standardization of assessments and compliance with all ISPS requirements. The Port Security Risk Assessment Tool (PSRAT) was used to provide additional standardization and consistency and aid in the development of the PFSAs. The PFSA was then submitted to the appropriate Coast Guard District Commander for review prior to December 1, 2003. Following the District Commander review it was submitted to the appropriate Area Commander for approval all PFSA's were approved prior to May 31, 2004.

The facility owner or operator within the port facility were required to perform a FSA ensuring that the following background information, if applicable, was provided to the person or persons conducting the assessment. Facilities were provided an assessment tool that could be used to assist them in development of their FSA:

1. The general layout of the facility, including:
    - The location of each active and inactive access point to the facility;
    - The number, reliability, and security duties of facility personnel;
    - Security doors, barriers, and lighting;
    - The location of restricted areas;
    - The emergency and stand-by equipment available to maintain essential services;
    - The maintenance equipment, cargo spaces, storage areas, and unaccompanied baggage storage;
    - Location of escape and evacuation routes and assembly stations; and
    - Existing security and safety equipment for protection of personnel and visitors.

2. Response procedures for fire or other emergency conditions;
3. Procedures for monitoring facility and vessel personnel, vendors, repair technicians, and dock workers;
4. Existing contracts with private security companies and existing agreements with local or municipal agencies;
5. Procedures for controlling keys and other access prevention systems;
6. Procedures for cargo and vessel stores operations;
7. Response capability to security incidents;
8. Threat assessments, including the purpose and methodology of the assessment, for the port in which the facility is located or at which passengers embark or disembark;
9. Previous reports on security needs; and

10. Any other existing security procedures and systems, equipment, communications, and facility personnel.

On-scene survey. The facility owner or operator ensured that an on-scene survey of each facility was conducted. The on-scene survey examined and evaluated existing facility protective measures, procedures, and operations to verify or collect the information required. The on-scene survey is one of the keys components in the development of the Facility Security Assessments (FSA)

Analysis and recommendations. While conducting the FSA, the facility owner or operator ensured that the FSO analyzed the facility background information and the on-scene survey, and considered the requirements, provided recommendations to establish and prioritize the security measures included in the FSP. The analysis considered;

1. Each vulnerability found during the on-scene survey including but not limited to:

- Waterside and shore-side access to the facility and vessel berthing at the facility;
- Structural integrity of the piers, facilities, and associated structures;
- Existing security measures and procedures, including identification systems;
- Existing security measures and procedures relating to services and utilities;
- Measures to protect radio and telecommunication equipment, including computer systems and networks;
- Adjacent areas that may be exploited during or for an attack;
- Areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations within the facility;
- Existing agreements with private security companies providing waterside and shore-side security services;
- Any conflicting policies between safety and security measures and procedures;
- Any conflicting facility operations and security duty assignments;
- Any enforcement and personnel constraints;
- Any deficiencies identified during daily operations or training and drills; and
- Any deficiencies identified following security incidents or alerts, the report of security concerns, the exercise of control measures, or audits;

2. Possible security threats, including but not limited to:

- Damage to or destruction of the facility or of a vessel moored at the facility;
- Hijacking or seizure of a vessel moored at the facility or of persons on board;
- Tampering with cargo, essential equipment or systems, or stores of a vessel moored at the facility;
- Unauthorized access or use including the presence of stowaways;
- Smuggling dangerous substances and devices to the facility;
- Use of a vessel moored at the facility to carry those intending to cause a security incident and their equipment;

- Use of a vessel moored at the facility as a weapon or as a means to cause damage or destruction;
- Impact on the facility and its operations due to a blockage of entrances, locks, and approaches; and
- Use of the facility as a transfer point for nuclear, biological, radiological, explosive, or chemical weapons;

3. Threat assessments by Government agencies; Vulnerabilities, including human factors, in the facility's infrastructure, policies and procedures;

4. Any particular aspects of the facility, including the vessels using the facility, which make it likely to be the target of an attack;

5. Likely consequences in terms of loss of life, damage to property, and economic disruption, including disruption to transportation systems, of an attack on or at the facility; and

6. Locations where access restrictions or prohibitions will be applied for each MARSEC Level.

7. The facility owner or operator ensured that a written FSA report was prepared and included as part of the PFSP. The report contained:

- A summary of how the on-scene survey was conducted;
- A description of existing security measures, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems;
- A description of each vulnerability found during the on-scene survey;
- A description of security measures that could be used to address each vulnerability;
- A list of the key facility operations that are important to protect; and
- A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the facility.
- A PFSA report must describe the following elements within the facility:
- Physical security;
- Structural integrity;
- Personnel protection systems;
- Procedural policies;
- Radio and telecommunication systems, including computer systems and networks;
- Relevant transportation infrastructure; and utilities.

8. The FSA report listed the persons, activities, services, and operations that were important to protect, in each of the following categories:

- Facility personnel;
- Passengers, visitors, vendors, repair technicians, vessel personnel, etc.;
- Capacity to maintain emergency response;
- Cargo, particularly dangerous goods and hazardous substances;
- Delivery of vessel stores;
- Any facility security communication and surveillance systems; and
- Any other facility security systems, if any.

9. The FSA report accounted for vulnerabilities in the following areas:
   - Conflicts between safety and security measures;
   - Conflicts between duties and security assignments;
   - The impact of watch-keeping duties and risk of fatigue on facility personnel alertness and performance;
   - Security training deficiencies; and
   - Security equipment and systems, including communication systems.

10. The FSA report discussed and evaluated key facility measures and operations, including:

   - Ensuring performance of all security duties;
   - Controlling access to the facility, through the use of identification systems or otherwise;
   - Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);
   - Procedures for the handling of cargo and the delivery of vessel stores;
   - Monitoring restricted areas to ensure that only authorized persons have access;
   - Monitoring the facility and areas adjacent to the pier; and
   - The ready availability of security communications, information, and equipment.

A completed FSA report was required to be submitted on or before December 31, 2003. Owners or operators of facilities not in service on or before December 31, 2003, were required to comply 60 days prior to beginning operations or by December 31, 2003, whichever was later.

The owner or operator of each facility in operation was required to submit one copy of the FSA report with their Facility Security Plan (FSP) that is centrally reviewed in a three-stage review process, with Stage III review and approval conducted by the cognizant U. S. Coast Guard Captain of the Port (COTP/PFSO).

The Stage I review ensured that the eighteen basic required sections are properly included and/or addressed within the FSP. Stage II review was an in depth review of the eighteen basic required sections ensuring the FSP that contains all the regulatory requirements contained in 33CFR105.

During Stage III, the cognizant COTP examined each submission for compliance and either:

1. Approved it and specified any conditions of approval, returned it to the submitter with a letter stating its acceptance and any conditions;

2. Returned it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or

3. Disapproved it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

A FSA that is approved by the cognizant COTP as part of the FSP is valid for five years from the date of its approval.

What minimum skills are required for persons conducting PFSA's? (ISPS Code section A/15.3)

Those involved in a PFSA and were required to be able to draw upon expert assistance in the following areas, as appropriate:
(1) Knowledge of current security threats and patterns;
(2) Recognition and detection of dangerous substances and devices;
(3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
(4) Techniques used to circumvent security measures;
(5) Methods used to cause a security incident;
(6) Effects of dangerous substances and devices on structures and facility services;
(7) Facility security requirements;
(8) Facility and vessel interface business practices;
(9) Contingency planning, emergency preparedness, and response;
(10) Physical security requirements;
(11) Radio and telecommunications systems, including computer systems and networks;
(12) Marine or civil engineering; and
(13) Facility and vessel operations.

Are PFSA's used for each Port Facility Security Plan? (ISPS Code section A/15.1)

Yes, each PFSP and FSP required an assessment.

Do single PFSA's cover more than one port facility? (ISPS Code section A/15.6)

No, a separate PFSA was used for each PFSP.

A facility owner or operator within the designated port facility could generate and submit a single FSA for more than one facility to the extent that they share similarities in design and operations, if authorized and approved by the cognizant COTP/PFSO.

Who is responsible for informing the IMO if the single PFSA covers more than one port facility? (ISPS Code section A/15.6)

For the United States, no single PFSA covered more than one port facility.

What national guidance has been developed to assist with the completion of PFSA's? (SOLAS regulation XI2/10.2.1)

Navigation and Vessel Inspection Circular (NVIC) No. 03-03 was written guidance for facilities that were mandated to complete a PFSA under MTSA. The NVIC included step-by-step instructions on completing a PFSA.

What procedures are in place for determining when re-assessment takes place? (ISPS Code section A/15.4)

The facility must ensure that an audit of the PFSP which includes the PFSA is performed annually, beginning no later than one year from the initial date of approval, and attach a letter to the PFSP certifying that the PFSP meets the applicable requirements.

Further, the FSP must be audited if there is a change in the facility's ownership or operator, or if there have been modifications to the facility, including but not limited to physical structure, emergency response procedures, security measures, or operations. Auditing the FSP as a result of modifications to the facility may be limited to those sections of the FSP affected by the facility modifications. Unless impracticable due to the size and nature of the company or the facility, personnel conducting internal audits of the security measures specified in the FSP or evaluating its implementation must:

- Have knowledge of methods for conducting audits and inspections, and security, control, and monitoring techniques;
- Not have regularly assigned security duties; and
- Be independent of any security measures being audited.

If the results of an audit require amendment of either the FSA or FSP, the FSO must submit the amendments to the cognizant COTP/PFSO for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended FSP meets the applicable requirements of this part.

The cognizant COTP/PFSO upon a determination that an amendment is needed to maintain the facility's security. The cognizant COTP/PFSO, who will give the facility owner or operator written notice, will request that the facility owner or operator propose amendments addressing any matters specified. The facility owner or operator will have at least 60 days to submit its proposed amendments.

An approved FSP is valid for five years from the date of its approval.

What procedures are in place for protecting the PFSA's from unauthorized access or disclosure? (ISPS Code section A/15.7)

All PFSA's and FSA's are considered Sensitive Security Information (SSI) and are required to be stored and handled in accordance with 49 CFR 1520. As such they are protected from disclosure under the United States Freedom of Information Act.

Port Facility Security Plans (PFSP's)

How are Port Facility Security Officers designated? (ISPS Code section A/17.1)

The United States MTSA regulations designated the COTP as the Federal Maritime Security Coordinator (FMSC). In this role, the COTP/FMSC assumes all the responsibilities as the ISPS Code Port Facility Security Officer (PFSO)

Each owner or operator within the port facility designated a Company Security Officer (CFO) and a facility Security Officer (FSO) for their facility. The same person may serve as the FSO for more than one facility, provided the facilities are in the same COTP/FMSC zone and are not more than 50 miles apart. If a person serves as the FSO for more than one facility, the name of each facility for which he or she is the FSO must be listed in the FSP of each facility for which or she is the FSO.

What are the minimum training requirements that have been set by the contracting government for PFSO's? (ISPS Code section A/18.8)

The PFSO and FSO must have general knowledge, through training or equivalent job experience, in the following:

- Security organization of the facility;
- General vessel and facility operations and conditions;
- Vessel and facility security measures, including the meaning and the requirements of the different MARSEC Levels;
- Emergency preparedness, response, and contingency planning;
- Security equipment and systems, and their operational limitations; and
- Methods of conducting audits, inspections, control, and monitoring techniques.
- Relevant international laws and codes, and recommendations;
- Relevant government legislation and regulations;
- Responsibilities and functions of local, State, and Federal law enforcement agencies;
- Security assessment methodology;
- Methods of facility security surveys and inspections;
- Instruction techniques for security training and education, including security measures and procedures;
- Handling sensitive security information and security related communications;

- Current security threats and patterns;
- Recognizing and detecting dangerous substances and devices;
- Recognizing characteristics and behavioral patterns of persons who are likely to threaten security;
- Techniques used to circumvent security measures;
- Conducting physical searches and non-intrusive inspections;
- Conducting security drills and exercises, including exercises with vessels; and
- Assessing security drills and exercises.

Are procedures used to determine the individuals/organizations responsible for the preparation of the PFSP? If yes please describe.

Responsibility for the preparation of the PFSP was delegated by the Commandant of the Coast Guard to each COTP, acting as the PFSO his/her port facility, defined by their AOR.

Each individual facility within the port facility to which MTSA was applicable was required prepare a FSO. The FSO was then submitted for approval by the COTP/PFSO.

Are procedures in place to protect PFSP's from unauthorized access? (ISPS Code sections A/16.7 and A/16.8)

All PFSP's and FSP'S are considered Sensitive Security Information (SSI). As such they are protected from disclosure under the United States Freedom of Information Act.

What procedures are in place for approval and subsequent amendments of the PFSP's (ISPS Code section A/16.6)?

Each Coast Guard COTP submitted a PFSP for his/her port facility under the guidance set by Commandant, U. S. Coast Guard, to insure a national standardization of assessments and compliance with all ISPS requirements. The PFSP was then submitted to the appropriate Coast Guard District Commander for review prior to December 1, 2003. Following the District Commander review it was submitted to the appropriate Area Commander for approval all PFSP's were approved prior to May 31, 2004.

Each individual facility within the port facility to which MTSA was applicable was required to submit a FSP to the appropriate COTP/PFSO for approval prior to January 1, 2004. The FSPs were reviewed using a three-stage process with cognizant COTP/PFSO conducting the final review and approval. Approved FSPs are valid for five years from the date of their approval.

An audit of the PFSP is performed annually, beginning no later than one year from the initial date of approval, and attach a letter to the PFSP certifying that the PFSP meets the applicable requirements.

Each individual facility within the port facility to which MTSA was applicable the FSP must be audited if there is a change in the facility's ownership or operator, or if there have been modifications to the facility, including but not limited to physical structure, emergency response procedures, security measures, or operations. Auditing the PFSP as a result of modifications to the facility may be limited to those sections of the PFSP affected by the facility modifications.

If the results of an audit require amendment of either the FSA or FSP, the FSO must submit the amendments to the cognizant COTP/FMSC for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended FSP meets the applicable requirements of this part.

The cognizant COTP/FMSC upon a determination that an amendment is needed to maintain the facility's security. The cognizant COTP/FMSC, who will give the facility owner or operator written notice, will request that the facility owner or operator propose amendments addressing any matters specified. The facility owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the facility owner or operator shall ensure temporary security measures are implemented to the satisfaction of the COTP/FMSC. Proposed amendments must be submitted to the cognizant COTP/FMSC. If initiated by the facility owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the cognizant COTP/FMSC allows a shorter period. The cognizant COTP/PFSO will approve or disapprove the proposed amendment.

Security Levels

Who is the authority responsible for setting the security level for port facilities? (SOLAS regulation XI-2/3.2)

The Commandant of the U.S. Coast Guard will set the Security Level consistent with the equivalent U.S. Department of Homeland Security Advisory System. The Commandant retains discretion to adjust the Security Level when necessary to address any particular security concerns or circumstances related to the maritime elements of the national transportation system. The Captain of the Port for each region of the United States may temporarily raise the Security Level for the port, a specific marine operation within the port, or a specific industry within the port, when necessary to address an exigent circumstance immediately affecting the security of the maritime elements of the transportation system in his/her area of responsibility.

The Security Levels are aligned with the U. S. Department of Homeland Security's Homeland Security Advisory System (HSAS),

Relation Between HSAS and Security Levels

Homeland security advisory system (HSAS) threat condition	Equivalent Security level
Low: Green.....	Security Level 1.
Guarded: Blue.....	
Elevated: Yellow.....	
High: Orange.....	Security Level 2.
Severe: Red.....	Security Level 3.

What are the procedures for communicating security levels to port facilities by the responsible authority? (SOLAS regulation XI-2/3.2)

Each FMSC formed an Area Maritime Security (AMS) Committee, which is comprised of the other Federal, state, and local agencies, as well as members of the local maritime industry, in their areas of responsibility. These Committees are enhancing the exchange of communications between the Coast Guard and local agencies and the maritime stakeholders.

Unless otherwise directed, each port, vessel, and facility shall operate at Security Level One. COTP will;

1. Communicate any changes in the Security Levels through a local Broadcast Notice to Mariners, an electronic means, if available, or as detailed in the Area Maritime Security Plan for each COTP Zone.

2. Communication of threats. When the COTP is made aware of a threat that may cause a transportation security incident, the COTP will, when appropriate, communicate to the port stakeholders, vessels, and facilities in his or her area of responsibility the following details:

- Geographic area potentially impacted by the probable threat;
- Any appropriate information identifying potential targets;
- Onset and expected duration of probable threat;
- Type of probable threat; and
- Required actions to minimize risk.

3. Attainment.

- Each owner or operator required to have a security plan must ensure confirmation to their local COTP the attainment of measures or actions described in their security plan and any other requirements imposed by the COTP that correspond with the Security Level being imposed by the change.

- Each owner or operator required to have a security plan affected by a change in the Security Level must confirm to their cognizant COPT that security measures or actions described in their security plan have been implemented to reflect the security level being imposed.

What are the procedures for communicating port facilities' security levels to ships? (SOLAS regulations XI-2/4.3 and XI- 2/7.1)

When notified of an increase in the MARSEC Level, the facility owner and operator must ensure: Vessels moored to the facility and vessels scheduled to arrive at the facility within 96 hours of the MARSEC Level change are notified of the new Security Level and the Declaration of Security as necessary.

What are the contact points and procedures for receiving ships' security level information in the Contracting Government and for notifying ships of contact details? (SOLAS regulation XI-2/7.2)

Ships will provide notification of security level via the 96 Hour Advance Notice of Arrival. The information will be provided to the COTP through the vessels agent and the National Vessel Movement Center. U.S. Flagged vessels will be provided security levels through a Notice to Mariners.

Declaration of Security

What procedures are used to determine when a Declaration of Security is required? (SOLAS regulation XI-2/10.3, ISPS Code section a/5.1)

Each facility owner or operator must ensure procedures are established for requesting a Declaration of Security (DoS) and for handling DoS requests from a vessel.

1. At Security Level 1, a facility receiving a cruise ship or a manned vessel carrying Certain Dangerous Cargo, in bulk, must comply with the following:

- Prior to the arrival of a vessel to the facility, the Facility Security Officer (PFSO) and Master, Vessel Security Officer (VSO/SSO), or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of time the vessel is at the facility; and
- Upon the arrival of the vessel at the facility, the PFSO and Master, VSO/SSO, or their designated representative, must sign the written DoS.
- Neither the facility nor the vessel may embark or disembark passengers, nor transfer cargo or vessel stores until the DoS has been signed and implemented.
- At Security Levels 2 and 3, the PFSOs, or their designated representatives, of facilities interfacing with manned vessels must sign and implement a DoS.

- At Security Levels 1 and 2, PFSOs of facilities that frequently interface with the same vessel may implement a continuing DoS for multiple visits, provided that:
- The DoS is valid for a specific Security Level;
  1. The effective period at Security Level 1 does not exceed 90 days; and
  2. The effective period at Security Level 2 does not exceed 30 days.
- When the Security Level increases beyond that contained in the DoS, the continuing DoS is void and a new DoS must be executed in accordance with this section.
- A copy of all currently valid continuing DoSs must be kept with the Port Facility Security Plan.
- The COTP may require, at any time, at any Security Level, any facility subject to this part to implement a DoS with the VSO/SSO prior to any vessel-to-facility interface when he or she deems it necessary.

At Security Level 1, the Master or Vessel Security Officer (VSO/SSO), or their designated representative, of any cruise ship or manned vessel carrying Certain Dangerous Cargoes, in bulk, must complete and sign a DoS with the VSO/SSO or Port Facility Security Officer (PFSO), or their designated representative, of any vessel or facility with which it interfaces.

- For a vessel-to-facility interface, prior to arrival of a vessel to a facility, the PFSO & Master, SSO, or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of time the vessel is at the facility. Upon a vessel's arrival to a facility and prior to any passenger embarkation or disembarkation or cargo transfer operation, the PFSO or Master, SSO, or designated representatives must sign the written DoS.

- For a vessel engaging in a vessel-to-vessel activity, prior to the activity, the respective Masters, SSOs, or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of the vessel-to-vessel activity. Upon the vessel-to-vessel activity and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, SSOs, or designated representatives must sign the written DoS.

- At Security Levels 2 & 3, the Master, SSO, or designated representative of any manned vessel required to comply with this part must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of the vessel-to-vessel activity. Upon the vessel-to-vessel activity and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, SSOs, or designated representatives must sign the written DoS.

- At Security Levels 2 and 3, the Master, SSO, or designated representative of any manned vessel required to comply with this part must coordinate security needs and procedures, and agree upon the contents of the DoS for the period the vessel is at the facility. Upon the vessel's arrival to a facility and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective PFSO and Master, SSO, or designated representatives must sign the written DoS.

- At Security Levels 1 and 2, SSOs of vessels that frequently interface with the same facility may implement a continuing DoS for multiple visits, provided that:
    1. The DoS is valid for the specific Security Level;
    2. The effective period at Security Level 1 does not exceed 90 days; and
    3. The effective period at Security Level 2 does not exceed 30 days.

When the MARSEC Security Level increases beyond the level contained in the DoS, the continuing DoS becomes void and a new DoS must be signed and implemented in accordance with this section.

The COTP may require at any time, at any Security Level, any manned vessel subject to this part to implement a DoS with the SSO or PFSO prior to any vessel-to-vessel activity or vessel-to-facility interface when he or she deems it necessary.
The COTP may also require a DoS be completed for vessels and facilities during periods of critical port operations, special marine events, or when vessels give notification of a higher MARSEC Level than that set in the COTP's Area of Responsibility

What is the minimum time frame that a Declaration of Security is retained? (ISPS Code section A/5.6)

Owners and Operators within the port facility must keep a copy of all currently valid continuing DoSs with their FSP.

Declaration of Security (DoS) on manned vessels must keep on board a copy of the last 10 DoSs and a copy of each continuing DoS for at least 90 days after the end of its effective period.

Delegation of Tasks and Duties

What tasks and duties have the contracting governments delegated to Recognized Security Organizations (RSOs) or others? (ISPS Code section A/4.3)

The United States has not delegated any tasks or duties to any Recognized Security Organization. The United States Coast Guard (USCG) as Designated Authority and the lead agency for maritime homeland security has been assigned the task of implementing the ISPS Code and enforcing its requirements under the Maritime Transportation Security Act of 2002.

To whom have these tasks and duties been delegated? What oversight procedures are in place (SOLAS regulation XI-2/13.2)?

It has not been delegated.

DEFINITIONS:

Unless otherwise specified:

Alternative Security Program: a third-party or industry organization developed standard that the Commandant has determined provides an equivalent level of security.
Area Commander: U.S. Coast Guard officer designated by the Commandant to command a Coast Guard Area as described in 33 CFR part 3. There is one Atlantic Area Commander and one Pacific Area Commander, whose operational commands are divided by geographic boundaries.
Area Maritime Security (AMS) Assessment: an analysis that examines and evaluates the infrastructure and operations of a port taking into account possible threats, vulnerabilities, and existing protective measures, procedures and operations.
Area Maritime Security (AMS) Committee: Port Security Committee established pursuant to Navigation and Vessel Inspection Circular (NVIC) 09-02, available from the cognizant Captain of the Port (COTP) or at http://www.uscg.mil/hq/g-m/nvic.
Area of Responsibility (AOR): a Coast Guard area, district, marine inspection zone or COTP zone described in 33 CFR part 3.
Audit: an evaluation of a security assessment or security plan performed by an owner or operator, the owner or operator's designee, or an approved third-party, intended to identify deficiencies, non-conformities and/or inadequacies that would render the assessment or plan insufficient.
Barge: a non-self-propelled vessel.
Barge fleeting facility: a commercial area, subject to permitting by the Army Corps of Engineers, as provided in 33 CFR part 322, part 330, or pursuant to a regional general permit the purpose of which is for the making up, breaking down, or staging of barge tows.
Breach of security: an incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated.
Bulk or in bulk: a commodity that is loaded or carried on board a vessel without containers or labels, and that is received and handled without mark or count.
Captain of the Port (COTP): the local officer exercising authority for the COTP zones described in 33 CFR part 3. The COTP is the Federal Maritime Security Coordinator and also the Port Facility Security Officer as described in the ISPS Code, part A.
Cargo: any goods, wares, or merchandise carried, or to be carried, for consideration, whether directly or indirectly flowing to the owner, charterer, operator, agent, or any other person interested in the vessel, facility, or OCS facility, except dredge spoils.
Cargo vessel: a vessel that carries, or intends to carry, cargo as defined in this section.
Certain Dangerous Cargo (CDC): the same as defined in 33 CFR 160.204.

Commandant: the Commandant of the U.S. Coast Guard.
Company: any person or entity that owns any facility, vessel, or OCS facility subject to the requirements of 33 CFR parts 103-106, or has assumed the responsibility for operation of any facility, vessel, or OCS facility subject to these requirements, including the duties and responsibilities imposed by 33 CRF parts 103-106.
Company Security Officer (CSO): the person designated by the Company as responsible for the security of the vessel or OCS facility, including implementation and maintenance of the vessel or OCS facility security plan, and for liaison with their respective vessel or facility security officer and the Coast Guard.
Contracting Government: any government of a nation that is a signatory to SOLAS, other than the U.S.
Cruise ship: any vessel over 100 gross register tons, carrying more than 12 passengers for hire which makes voyages lasting more than 24 hours, of which any part is on the high seas. Passengers from cruise ships are embarked or disembarked in the U.S. or its territories. Cruise ships do not include ferries that hold Coast Guard Certificates of Inspection endorsed for ``Lakes, Bays, and Sounds'', that transit international waters for only short periods of time on frequent schedules.
Dangerous goods and/or hazardous substances: cargoes regulated by 33 CFR 126, 127, or 154
Dangerous substances or devices: any material, substance, or item that reasonably has the potential to cause a transportation security incident.
Declaration of Security (DoS): an agreement executed between the responsible Vessel and Facility Security Officer, or between Vessel Security Officers in the case of a vessel-to-vessel activity, that provides a means for ensuring that all shared security concerns are properly addressed and security will remain in place throughout the time a vessel is moored to the facility or for the duration of the vessel-to-vessel activity, respectively.
District Commander: the U.S. Coast Guard officer designated by the Commandant to command a Coast Guard District described in 33 CFR part 3.
Drill: a training event that tests at least one component of the AMS, vessel, or facility security plan and is used to maintain a high level of security readiness.
Exercise: a comprehensive training event that involves several of the functional elements of the AMS, vessel, or facility security plan and tests communications, coordination, resource availability, and response.
Facility Security Assessment (FSA): an analysis that examines and evaluates the infrastructure and operations of the facility taking into account possible threats, vulnerabilities, consequences, and existing protective measures, procedures and operations.
Facility Security Officer (FSO): the person designated as responsible for the development, implementation, revision and maintenance of the facility security plan and for liaison with the COTP and Company and Vessel Security Officers.
Facility Security Plan (FSP): the plan developed to ensure the application of security measures designed to protect the facility and its servicing vessels or those vessels interfacing with the facility, their cargoes, and persons on board at the respective MARSEC Levels.

Ferry: a vessel which is limited in its use to the carriage of deck passengers or vehicles or both, operates on a short run on a frequent schedule between two or more points over the most direct water route, other than in ocean or coastwise service.
Foreign vessel: a vessel of foreign registry or a vessel operated under the authority of a country, except the U.S., that is engaged in commerce.
Hazardous materials: hazardous materials subject to 46 CFR parts 148, 150, 151, 153, or 154, or 49 CFR parts 171 through 180.
Infrastructure: facilities, structures, systems, assets, or services so vital to the port and its economy that their disruption, incapacity, or destruction would have a debilitating impact on defense, security, the environment, long-term economic prosperity, public health or safety of the port.
International voyage: a voyage between a country to which SOLAS applies and a port outside that country. A country, as used in this definition, includes every territory for the internal relations of which a contracting government to the convention is responsible or for which the United Nations is the administering authority. For the U.S., the term ``territory'' includes the Commonwealth of Puerto Rico, all possessions of the United States, and all lands held by the U.S. under a protectorate or mandate. Vessels solely navigating the Great Lakes and the St. Lawrence River as far east as a straight line drawn from Cap des Rosiers to West Point, Anticosti Island and, on the north side of Anticosti Island, the 63rd meridian, are considered on an ``international voyage'' when on a voyage between a U.S. port and a Canadian port.
ISPS Code: the International Ship and Port Facility Security Code, as incorporated into SOLAS.
Maritime Security (MARSEC) Directive: an instruction issued by the Commandant, or his/her delegee, mandating specific security measures for vessels and facilities that may be involved in a transportation security incident.
Maritime Security (MARSEC) Level: the level set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the U.S.
MARSEC Level 1: the level for which minimum appropriate protective security measures shall be maintained at all times.
MARSEC Level 2: the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident.
MARSEC Level 3: the level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable or imminent, although it may not be possible to identify the specific target.
OCS Facility: any artificial island, installation, or other complex of one or more structures permanently or temporarily attached to the subsoil or seabed of the OCS, erected for the purpose of exploring for, developing or producing oil, natural gas or mineral resources. This definition includes all mobile offshore drilling units (MODUs) not covered under 33 CFR 104, when attached to the subsoil or seabed of offshore locations, but does not include deepwater ports, as defined by 33 U.S.C. 1502, or pipelines.

Owner or operator: any person or entity that owns, or maintains operational control over, any facility, vessel, or OCS facility. This includes a towing vessel that has operational control of an unmanned vessel when the unmanned vessel is attached to the towing vessel and a facility that has operational control of an unmanned vessel when the unmanned vessel is not attached to a towing vessel and is moored to the facility; attachment begins with the securing of the first mooring line and ends with the casting-off of the last mooring line.

Passenger vessel:

(1) On an international voyage, a vessel carrying more than 12 passengers, including at least one passenger-for-hire; and

(2) On other than an international voyage:

(i) A vessel of at least 100 gross register tons carrying more than 12 passengers, including at least one passenger-for-hire;

(ii) A vessel of less than 100 gross register tons carrying more than 6 passengers, including at least one passenger-for-hire;

(iii) A vessel that is chartered and carrying more than 12 passengers;

(iv) A submersible vessel that is carrying at least one passenger-for-hire; or

(v) A wing-in-ground craft, regardless of tonnage, that is carrying at least one passenger-for-hire.

Passenger-for-hire: a passenger for whom consideration is contributed as a condition of carriage on the vessel, whether directly or indirectly flowing to the owner, charterer, operator, agent, or any other person having an interest in the vessel.

Restricted areas: the infrastructures or locations identified in an area, vessel, or facility security assessment or by the operator that require limited access and a higher degree of security protection. The entire facility may be designated the restricted area, as long as the entire facility is provided the appropriate level of security.

Review and approval: the process whereby Coast Guard officials evaluate a plan or proposal to determine if it complies with this subchapter and/or provides an equivalent level of security.

Screening: a reasonable examination of persons, cargo, vehicles, or baggage for the protection of the vessel, its passengers and crew. The purpose of the screening is to secure the vital government interest of protecting vessels, harbors, and waterfront facilities from destruction, loss, or injury from sabotage or other causes of similar nature. Such screening is intended to ensure that dangerous substances and devices, or other items that pose a real danger of violence or a threat to security are not present.

Security system: a device or multiple devices designed, installed and operated to monitor, detect, observe or communicate about activity that may pose a security threat in a location or locations on a vessel or facility.

Sensitive security information (SSI): information within the scope of 49 CFR part 1520.

SOLAS: the International Convention for the Safety of Life at Sea Convention, 1974, as amended.

Survey: an on-scene examination and evaluation of the physical characteristics of a vessel or facility, and its security systems, processes, procedures, and personnel.

Vessel-to-facility interface: the interaction that occurs when a vessel is directly and immediately affected by actions involving the movement of persons, cargo, vessel stores, or the provisions of facility services to or from the vessel.

Vessel-to-port interface: the interaction that occurs when a vessel is directly and immediately affected by actions involving the movement of persons, cargo, vessel stores, or the provisions of port services to or from the vessel.