

LECTURE 6

6.0. PORT FACILITY AND PERSONNEL SECURITY

PORT FACILITY SECURITY OFFICER (FSO)

The Port Facility Security Officer (FSO) serves as the primary figure responsible for planning and overseeing the security operations of the port. While the FSO may also hold the title of Chief Security Officer, separating these roles is often recommended. This distinction allows the FSO to focus on the day-to-day security operations of the port, while the Chief Security Officer may handle broader administrative responsibilities unrelated to operational security.

In ports with diverse operations, such as those managing both passenger and cargo activities or mixed-use facilities, government security agencies often engage directly with the FSO. These agencies, like the U.S. Coast Guard (USCG), may require regular communication with the FSO to address potential risks and ensure compliance. A close operational connection between the FSO and port management is essential for addressing evolving security needs and ensuring the port's security plan remains relevant.

The International Ship and Port Facility Security (ISPS) Code defines the FSO as the individual responsible for creating, implementing, maintaining, and revising the Facility Security Plan (FSP) and coordinating with Ship and Company Security Officers. Similarly, U.S. legislation under the Maritime Transportation Security Act (MTSA) outlines the FSO's duties, qualifications, and responsibilities in line with these international guidelines.

GENERAL DUTIES

FSOs may undertake multiple roles within a port, depending on the management structure. While some ports may designate the FSO as the head of the security team, others may delegate this responsibility to an individual reporting to the Chief Security Officer. Regardless of the structure, the FSO should maintain close working relationships with facility users and relevant enforcement agencies to effectively manage the FSP. FSOs can delegate security tasks to other personnel but retain ultimate responsibility for ensuring these duties are performed.

QUALIFICATIONS

FSOs must possess comprehensive knowledge of port security, which can be obtained through training or equivalent experience. Key areas of expertise include:

- Facility security organization and operations
- Vessel security measures and MARSEC (Maritime Security) Levels
- Emergency response planning
- Security systems, auditing, and inspection techniques
- Relevant international and national security laws and regulations

- Conducting risk assessments and physical inspections
- Security-related communication and handling sensitive information

FSOs must also stay informed about evolving threats, recognize potential risks, and effectively manage security drills and exercises. They should ensure familiarity with specific requirements like the Transportation Worker Identification Credential (TWIC) program.

RESPONSIBILITIES

Key responsibilities include:

- Overseeing security assessments and the development of the FSP.
- Conducting regular audits and updating security plans as needed.
- Ensuring personnel are trained and security measures are implemented effectively.
- Maintaining compliance with MARSEC Levels and coordinating responses to changes in security conditions.
- Managing security records and reports.
- Collaborating with local, state, and federal law enforcement agencies.

PORT FACILITY SECURITY PLAN (FSP)

The FSP outlines the security measures necessary to protect port operations, vessels, cargo, and personnel. A well-maintained and actively used FSP is essential for managing port security effectively. The FSP should be treated as a dynamic document, continually updated and tested to address identified risks and ensure alignment with broader security strategies.

STRUCTURE OF THE FSP

Federal regulations mandate that port operators submit an FSP to the USCG for approval. While not required, it is beneficial to include a description of the facility, including its operations, workforce, and types of cargo and vessels handled.

The FSP should be detailed and user-friendly, serving as a comprehensive resource for current and future security personnel. Key sections typically include:

- Security administration and personnel training
- Records, drills, and exercises
- Security measures for access control, restricted areas, cargo handling, and monitoring
- Response plans for changes in MARSEC Levels
- Procedures for interfacing with vessels and completing Declarations of Security

MARITIME SECURITY (MARSEC) LEVELS

MARSEC Levels, established by the USCG, correspond to varying levels of security risk:

- **Level 1 (Normal):** Minimum security measures in place during standard operations.
- **Level 2 (Heightened):** Additional security measures implemented during periods of increased risk.
- **Level 3 (Exceptional):** Specific protective measures enforced when a security incident is imminent or has occurred.

MARSEC LEVEL ACTION PLANS

FSOs should prepare task lists for actions required during MARSEC Level changes. These plans may involve increasing screening procedures, coordinating with law enforcement, and enhancing patrols or inspections. Port-specific conditions and legal requirements should guide the development of these action plans.

Examples of tasks include:

- Communicating MARSEC Level changes to stakeholders and coordinating response efforts.
- Updating Declarations of Security with vessels.
- Increasing inspections of vehicles, piers, and cargo.
- Assigning additional security personnel during heightened alert levels.

By actively maintaining the FSP and adhering to MARSEC Level guidelines, ports can better address potential threats and ensure the safety of their operations.

FACILITY SECURITY ASSESSMENT (FSA)

A Facility Security Assessment (FSA) involves a comprehensive evaluation of a facility's infrastructure, operations, systems, and procedures to assess its current security posture. This process typically includes on-site surveys, analysis of gathered data, and the identification of vulnerabilities and potential threats. As outlined in the Maritime Transportation Security Act (MTSA) regulations, an FSA examines infrastructure, operations, threats, vulnerabilities, consequences, and existing protective measures. The outcome of the FSA is a written report that serves as a foundational element for the Facility Security Plan (FSP).

The assessment process includes several key components:

- **Assets and Infrastructure:** Identifying critical assets and evaluating their importance.
- **Threat Analysis:** Considering potential risks and adversaries.
- **Countermeasures and Procedures:** Reviewing existing protective measures.
- **Vulnerability Assessment:** Identifying weaknesses that could be exploited.

To ensure an impartial and effective evaluation, facility owners and operators may engage external consultants or third-party experts to conduct FSAs. This approach is particularly beneficial when addressing the financial and operational concerns of stakeholders.

» Expertise Required for FSAs

Individuals conducting FSAs should possess expertise in areas such as:

- Current security threats and detection of dangerous substances or devices.
- Behavioral analysis of individuals posing security risks.
- Methods to bypass security measures and cause incidents.
- Structural, marine, and civil engineering considerations.
- Physical security, emergency response planning, and contingency procedures.
- Radio, telecommunications, and IT systems relevant to facility operations.
- Facility-vessel interface and operational practices.

Additionally, the FSA and its associated reports must remain confidential to prevent unauthorized access or disclosure.

BACKGROUND INFORMATION

The FSA begins with gathering detailed background information, including:

- Facility layout, access points, restricted areas, and security equipment.
- Emergency response procedures and available equipment.
- Procedures for monitoring personnel, vendors, and dockworkers.
- Contracts with security providers and agreements with local authorities.
- Access control protocols for keys and other systems.
- Operations for cargo and vessel stores.
- Threat assessments and historical reports on security needs.

ON-SITE SURVEY

An on-site survey is conducted to evaluate existing security measures, operational procedures, and vulnerabilities. The findings are used to validate or expand upon the background information.

ANALYSIS AND RECOMMENDATIONS

The collected data is analyzed to identify vulnerabilities, assess potential threats, and recommend security improvements. This analysis includes:

- Reviewing access control for waterside and shore-side areas.
- Evaluating the structural integrity of piers and associated facilities.
- Identifying weaknesses in existing security measures, utilities, and IT systems.
- Assessing adjacent areas for potential exploitation.

- Examining conflicts between safety and security protocols.
- Considering human factors, such as personnel constraints and training deficiencies.

The analysis also evaluates possible threats, including:

- Damage to facilities or vessels.
- Unauthorized access or tampering.
- Use of the facility for smuggling or transporting dangerous substances.
- Disruptions to operations caused by blockages or attacks.

» Facility Security Assessment Report

The final FSA report, which is submitted alongside the FSP for approval, must include:

- A summary of the on-site survey methodology.
- Details of existing security measures and identified vulnerabilities.
- Recommendations to address each vulnerability.
- Lists of critical operations and personnel to protect.
- An evaluation of infrastructure, procedures, and communication systems.
- Identification of deficiencies in training, equipment, and operations.

» Facility Security Plan Audit

Under the MTSA, port facilities are required to conduct annual audits of their FSPs. These audits must:

- Be performed by individuals without regular security responsibilities at the facility.
- Identify deficiencies and ensure compliance with federal requirements.

Facilities may use internal resources, external agencies, or contracted consultants to conduct these audits. When engaging external parties, the scope of services should be clearly defined, and compliance with MTSA regulations must be ensured.

PORT PERSONNEL SECURITY AWARENESS

A key responsibility of the Facility Security Officer (FSO) at a port is to foster a security-conscious mindset among all employees, contractors, and visitors. Building awareness of security issues helps ensure a safe and resilient operational environment, aligning with regulatory standards like the Maritime Transportation Security Act (MTSA). A comprehensive security awareness strategy strengthens the port's ability to detect and mitigate threats, particularly in the face of global terrorism risks, by promoting collaboration across all levels of the workforce and stakeholder community.

A robust security awareness program should aim to:

- Provide foundational knowledge of port security to employees and port users.

- Highlight the importance of cultivating a culture of vigilance and security within port operations.
- Explain the relationship between vulnerabilities, risks, and the role of stakeholders in mitigating these risks.
- Demonstrate actionable steps that individuals can take to enhance the port's security infrastructure.

By empowering personnel with security knowledge and fostering collaboration, the port enhances its ability to identify, respond to, and prevent security threats. Training programs should cover recognizing criminal behaviors, identifying suspicious activity, and responding to safety concerns, forming a vital component of the port's layered security approach.

Port security depends on collective responsibility, with all stakeholders contributing to its safety and success. This shared accountability ensures the port's ongoing viability, supports international trade, and safeguards public safety.

OBJECTIVES OF A PORT SECURITY AWARENESS PROGRAM

Security awareness initiatives must emphasize that security is a shared responsibility across all levels of port operations. Training should address the following goals:

- 1. Promote a Security Culture:** Encourage awareness of potential threats to port assets and operations. A vigilant workforce helps identify risks and strengthens the overall security framework.
- 2. Maintain Commerce Flow:** By ensuring security awareness, the uninterrupted movement of goods and vessels can be preserved, supporting global trade.
- 3. Deter Terrorist Threats:** Prevent potential terrorist activities that could disrupt commerce and port operations by fostering cooperation between port users and security teams.
- 4. Prevent and Detect Criminal Activity:** Internal conspiracies or organized crime can undermine port security. All personnel should work to identify and eliminate such risks.
- 5. Control Access:** Ensure unauthorized individuals or vehicles do not enter restricted areas, enhancing the port's security posture.
- 6. Enable Threat Reporting:** Equip personnel to recognize and report suspicious behaviors, individuals, or cargo promptly.

KEY COMPONENTS OF A SECURITY AWARENESS PROGRAM

To effectively address potential security risks, port personnel must be trained in the following areas:

- 1. General Awareness:** Understand the importance of security and the role each individual plays in maintaining it.
- 2. Recognizing Threats:**

//

- **Crime:** Report suspicious activities, such as unusual behavior, unauthorized access attempts, or unexpected cargo.
 - **Terrorism:** Be informed about potential threats, stay aware of security levels (e.g., MARSEC Levels), and follow relevant protocols.
- 3. Security Procedures and Emergency Responses:** Know access requirements, credentialing processes, and emergency procedures.
 - 4. Communication Protocols:** Establish clear communication channels to report concerns and share critical updates.
 - 5. Restricted Access Areas:** Adhere to access restrictions and report unauthorized entries.
 - 6. Visitor Management:** Follow established procedures for escorting and verifying visitors.
 - 7. Cybersecurity:** Protect sensitive digital information from unauthorized access or disclosure.
 - 8. Weapons and Firearms:** Understand and comply with restrictions on bringing weapons onto port property.
 - 9. Emergency Plans:** Familiarize personnel with evacuation routes, bomb threat procedures, and natural disaster response plans.
 - 10. Contingency Planning:** Adapt operations to maintain functionality during disruptions, such as gate closures or changes in vessel schedules.
 - 11. Rules and Compliance:** Follow established guidelines, including credential checks and operational hours, and report violations.
 - 12. Threat Indicators:**
 - Identify suspicious individuals, such as those dressed unusually for the weather or acting erratically.
 - Report unauthorized photography of critical infrastructure.
 - 13. Knowledge of the Port:** Understand the port's layout to facilitate clear communication and efficient incident response.
 - 14. Training and Drills:** Participate in regular exercises to enhance familiarity with security plans and procedures.

// SUMMARY //

The FSO plays a central role in developing and managing the port's security framework, ensuring compliance with regulations such as the MTSA. Security awareness programs are essential to fostering a culture of vigilance, enhancing threat detection, and supporting effective responses to emergencies. By implementing these programs, ports can protect their infrastructure, facilitate international commerce, and create a secure environment for all stakeholders.

The success of port security lies in proactive planning, ongoing training, and the collective efforts of employees, contractors, and visitors. This collaborative approach is vital for maintaining the integrity of operations and safeguarding against evolving threats.