Professional Certificate in Global Maritime Regulatory Compliance

International Ship and Port Facility Security (ISPS) Code Compliance

International Ship and Port Facility Security (ISPS) Code Compliance

The International Ship and Port Facility Security (ISPS) Code is a comprehensive set of measures aimed at enhancing the security of ships and port facilities around the world. It was adopted by the International Maritime Organization (IMO) in response to the terrorist attacks of September 11, 2001, and came into effect on July 1, 2004.

The ISPS Code applies to all ships engaged in international voyages and all port facilities that receive ships engaged in international voyages. It sets out a number of mandatory requirements for both ships and port facilities to ensure the security of maritime transportation and prevent acts of terrorism.

Key Terms and Vocabulary:

1. Ship Security Officer (SSO): The SSO is responsible for the implementation and maintenance of the ship security plan on board a ship. They ensure that all security measures are in place and that the crew is properly trained to respond to security threats.

2. Port Facility Security Officer (PFSO): The PFSO is responsible for the implementation and maintenance of the port facility security plan at a port facility. They coordinate security activities, conduct security assessments, and ensure compliance with the ISPS Code.

3. Declaration of Security (DoS): A DoS is a formal agreement between the ship and the port facility detailing the security measures that will be implemented during a specific port call. It is used to ensure that both parties are aware of their respective security responsibilities.

4. Security Level: The ISPS Code defines three security levels (Security Level 1, 2, and 3) that reflect the degree of risk to maritime security. Each security level requires specific security measures to be implemented by ships and port facilities.

5. Ship Security Alert System (SSAS): The SSAS is a security system on board ships that enables the crew to alert the designated authorities in case of a security threat or breach. It is a key tool for enhancing the security of ships and ensuring a rapid response to security incidents.

6. Port Security: Port security refers to the measures and procedures implemented at port facilities to protect against security threats, such as terrorism, piracy, and smuggling. Port security includes access control, perimeter fencing, surveillance systems, and security patrols.

7. Security Assessment: A security assessment is a systematic evaluation of the security risks and

vulnerabilities facing a ship or port facility. It helps identify potential security threats and weaknesses and enables the development of effective security measures.

8. Security Plan: A security plan is a document that outlines the security measures and procedures to be implemented on board a ship or at a port facility. It includes details on access control, security drills, communications, and response to security incidents.

9. Security Drill: A security drill is a practice exercise conducted on board a ship or at a port facility to test the effectiveness of security procedures and the response of the crew or security personnel to a security threat. Security drills are essential for maintaining readiness and preparedness.

10. Security Incident: A security incident is an event that poses a threat to the security of a ship or port facility, such as a breach of security measures, unauthorized access, or suspicious activity. Security incidents must be reported and investigated promptly to prevent further threats.

11. Security Training: Security training is essential for all personnel on board a ship or working at a port facility to ensure they are aware of security risks and know how to respond to security threats. Training includes familiarization with security procedures, emergency response, and reporting suspicious activities.

12. Access Control: Access control refers to the measures implemented to control and monitor access to restricted areas on board a ship or at a port facility. This includes the use of identification cards, security gates, and surveillance systems to prevent unauthorized entry.

13. Security Equipment: Security equipment includes devices and systems used to enhance the security of ships and port facilities, such as CCTV cameras, metal detectors, X-ray scanners, and security alarms. Proper maintenance and testing of security equipment are essential for effective security measures.

14. Security Breach: A security breach is a violation of security measures that results in unauthorized access to a ship or port facility. Security breaches can compromise the safety of personnel and cargo and may lead to security incidents if not addressed promptly.

15. Contingency Plan: A contingency plan is a set of procedures and protocols to be followed in the event of a security incident or emergency at a ship or port facility. Contingency plans outline the steps to be taken to ensure the safety and security of personnel and assets.

16. Risk Assessment: Risk assessment is the process of identifying, analyzing, and evaluating security risks facing a ship or port facility. It helps determine the likelihood and impact of security threats and enables the implementation of appropriate security measures to mitigate risks.

17. Security Audit: A security audit is a formal review of the security measures and procedures in place on board a ship or at a port facility to assess compliance with the ISPS Code and identify areas for improvement. Security audits are conducted regularly to ensure ongoing compliance.

18. Security Culture: Security culture refers to the attitudes, beliefs, and behaviors of personnel towards security measures and procedures. A strong security culture is essential for maintaining vigilance, promoting

security awareness, and ensuring compliance with security requirements.

19. Security Incident Response: Security incident response is the process of reacting to and managing security incidents effectively to minimize their impact on the safety and security of a ship or port facility. Prompt and coordinated response is crucial for mitigating security threats.

20. Security Monitoring: Security monitoring involves the continuous observation and assessment of security measures and activities on board a ship or at a port facility to detect potential security threats or breaches. Effective security monitoring is essential for maintaining security readiness.

21. Security Communication: Security communication involves the exchange of information and instructions related to security measures and procedures between ships, port facilities, and security authorities. Clear and timely communication is essential for coordinating security efforts.

22. Security Incident Report: A security incident report is a formal document that details a security incident, including the nature of the incident, the date and time it occurred, the individuals involved, and the actions taken in response. Security incident reports are used for investigation and analysis.

23. Security Awareness: Security awareness refers to the knowledge and understanding of security risks, procedures, and responsibilities among personnel on board a ship or working at a port facility. Security awareness training is essential for promoting a culture of security vigilance.

24. Security Compliance: Security compliance refers to the adherence to the security measures and requirements set out in the ISPS Code by ships and port facilities. Compliance with security regulations is essential for ensuring the safety and security of maritime transportation.

25. Security Risk Management: Security risk management is the process of identifying, assessing, and mitigating security risks facing a ship or port facility. It involves implementing security measures to reduce the likelihood and impact of security threats on maritime operations.

26. Security Contingency: Security contingency refers to the backup plans and procedures to be followed in case of a security incident or emergency at a ship or port facility. Security contingencies enable a rapid and effective response to security threats to minimize their impact.

27. Security Alert: A security alert is a warning or notification of a potential security threat or breach that requires immediate action. Security alerts are issued to ships, port facilities, and security authorities to ensure a coordinated response to security incidents.

28. Security Assessment Report: A security assessment report is a formal document that summarizes the findings of a security assessment conducted on board a ship or at a port facility. The report outlines the security risks identified and recommends measures to enhance security.

29. Security Training Program: A security training program is a structured curriculum designed to educate personnel on board a ship or working at a port facility about security risks, procedures, and best practices. Security training programs are essential for building security awareness and readiness.

30. Security Incident Exercise: A security incident exercise is a simulated scenario conducted on board a ship or at a port facility to test the response of personnel to a security incident. Security incident exercises help evaluate the effectiveness of security procedures and identify areas for improvement.

By familiarizing yourself with these key terms and vocabulary related to International Ship and Port Facility Security (ISPS) Code Compliance, you will gain a better understanding of the security measures and procedures required to ensure the safety and security of maritime transportation. Proper implementation and compliance with the ISPS Code are essential for protecting ships, port facilities, personnel, and cargo from security threats and maintaining the integrity of the global maritime industry.