Port Facility Security Assessment 2024-2029

Pursuant to the Port Facility Security Assessment pursuant to Regulation (EC) No 725/2004 (ISPS)

Port Facility Name:

IMO Port Facility Number:

Port Facility Security Assessment 2024-2029. (PFSO to complete document information section below)

Title of Document uploaded to SSI:

Version number:

Date of Version:

Created by:

Description of Changes from previous version:

SECTION BELOW FOR COMPLETION BY MSO

Reviewed by:

Date of last review:

Approval Date:

Approved by:

Assessor Note: Each issue must have cover page completed including header section

Contents

Overview & Background 5
Scope 7
Review 7
Glossary & Definitions 7
Chapter 1 General Information 8
Chapter 1- 1.1 Assessment Team 9
Chapter 2 Port Facility General Information 10
Chapter 2 – 2.1 Port Facility General Information 11
Chapter 2 –2.1 Organisational Structure 12
Chapter2 – 2.2 Structural & Operational Information 14
Chapter 2 – 2.3 Tenants and adjacent users 15
Photos, Maps & Charts 16
Chapter 3 Port Facility Security Assessment 17
Chapter 3 – 3.1 Critical Assets 19
Chapter 3 – 3.2 important assets and infrastructure 21
Chapter 4 Port Facility Risk Assessment 23
Chapter 4 – 4.1 Risk Assessment 24
Chapter 5 Current Port Facility Security Measures 28
Chapter 5 – 5.1 Structural Port Facility Security Measures 30

Chapter 5 – 5.2 Procedural Port Facility Security Measures 31
Chapter 6 Port Facility Waterside Assessment 39
Overview 40
Chapter 6 – 6.2 Waterside General Information 41
Chapter 6 – 6.3 Waterside assets & infrastructure 43
Waterside Risk Analysis 45
Maps, Photos & charts of water approaches, berths, anchorages and manoeuvring areas. 46
Chapter 7 Report of RSO and Identification of Vulnerabilities & Recommendations 47
Checklist 50
Annex 51
1. Annex 1. List of Tenants and adjacent users 52
2. Annex 2. Report of RSO. (See Ch. 7) 54
3. Annex 3 55

Overview & Background

For the information of Port Facility Tenants and users, owners or operators of adjacent infrastructure

(Please refer to: Regulation EC/725/2004(4), ISPS Code 2004, Solas Chapter XI-2, Regulation 10, Irish S.I. 413/2004 EC & Port Facility Regulations)

On 31 March 2004 the European Parliament and the Council of the European Union adopted Regulation (EC) No 725/2004 [4] on enhancing ship and port facility security. The Regulation is limited in scope to security measures on board vessels ***and the immediate ship/port interface.***
The Regulation requires that the Port Facility Security Assessment is subject to a five year review, this is now occurring for the period 2024-2029, with compliance by all port facilities due by July 1st 2024.

This document – the Port Facility Security Assessment is required to be completed for every port facility including

In each assessment the following must be addressed:

- identification and evaluation of important assets and infrastructure which it is important to protect;
- identification of possible threats (including cyber threats) to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures;
- identification, selection and prioritisation of counter-measures and procedural changes and their level of effectiveness in reducing vulnerability; and
- identification of weaknesses, including human factors in the infrastructure, policies and procedures

.

Each port facility is responsible for undertaking its own port facility security assessment, using an approved Recognized Security Organization (RSO).
In multi facility port areas, the individual Port Facility Security Officers will liaise closely with the Port Security Officer in terms of organizing, completing, and uploading their Port Facility Security Assessments.

A waterside assessment module is included in the template and is to be completed for all port facilities in respect of the port ship interface area.

When carrying out port facility security assessments, RSO's and PFSO's should also take account of Section 7 of the European Commission MARSEC Doc. 9108 annex -Interim Guidance on Maritime Security for Member States' Competent Authorities.

All completed or amended port facility security assessments must be uploaded onto the Safe Seas Ireland (SSI) network by the PFSO. Comments/approvals of port facility assessments by the Administration will be posted via the SSI network. Documents submitted for final approval should have all tracked changes / comments removed.

On completion of the PFSA approval process, a Port Facility Security Plan is to be prepared and submitted to the SSI system for approval

Port Security Directive 2005/65/EC (information only)
In October 2005, the European Parliament and Council of the European Union adopted Directive 2005/65/EC on enhancing port security. The scope of the Directive extends back from the Ship/Shore interface into the greater port area, with Member States defining port boundaries as any specified area of land and water in which the port is situated containing works and equipment designed to facilitate commercial maritime transport operations. Ports may be multi facility or single facility entities. For the 2024 – 2029 period, the port authority will arrange for a separate single Port Security Assessment to be completed for each Port in accordance with Directive 2005/65/EC and this is completed utilising a different template. Whereas port facilities will no longer submit port security assessments to SSI, the port facilities are required by the regulations to co-operate with the PSO / RSO responsible for the carrying out of the separate Port Security Assessment , including both the landside and overall waterside security assessment.

Brian Hogan
Chief Surveyor
Irish Maritime Administration

Scope

The template will be used to assess the security of ALL port facilities defined by the Administration. The assessment will include the Ship/Shore interface security measures as per Regulation 725/2004.

Review

Member States have to ensure that port facility security assessments and port facility security plans are reviewed as appropriate. They shall be reviewed at least once every five years. Port companies are obliged to resubmit Port Facility Security Assessments in the event of any operational or procedural changes to a port facility which affects the basis on which the assessment was completed. E.g. A change from ro/ro cargo ship to ro/ro passenger ship operations would require a re-assessment.

Glossary & Definitions

Port: any specified area of land and water with boundaries defined by the Member State in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations.

Ship/Port interface: interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons or goods or the provision of port services to or from a ship.

Port Facility: location where the ship/port interface takes place. This includes areas such as anchorages, waiting berths and approaches from seaward.

Port Security Officer (PSO): A Port Security Officer shall be approved by the Member State as per Directive 2005/65 EC. Each port, where practical, shall have a different Port Security Officer, but may, if appropriate, share a Port Security Officer.

Port Facility Security Officer (PFSO): the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers as per Regulation 725/2004.

Port Facility Security Assessment: Each port facility security assessment shall be carried out taking into account as a minimum the detailed requirements laid down in Regulation 725/2004. Port facility security assessments may be carried out by a recognised security organisation. Port facility security assessments shall be approved by the member state concerned.

Security Level 1: the level for minimum appropriate protective security measures shall be maintained at all times

Security Level 2: the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of a heightened risk of a security incident

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

Chapter 1 General Information

1.1 Assessment Team

Chapter 1- 1.1 Assessment Team

No.	Reg 725/2004 (ISPS Code)	General Information – Assessment Team	
1		**Date of Assessment / Survey**	
2		**Name(s) of person(s) carrying out assessment**	
3	**Part B** **4.5**	**Relevant skills and expertise of assessors.**	
4	**Part B 15.8** **15.10** **15.12**	**Consultation with national Authorities relating to potential threats to facility**	Yes ☐ No☐ Give details: The RSO should liaise with An Garda Síochána to determine: .1 any particular aspects of the port facility, including the vessel traffic using the facility, which make it likely to be the target of an attack; .2 the likely consequences in terms of loss of life, damage to property

Chapter 2 Port Facility General Information

2.1 General Information & Organisational Structure

2.2 Port Facility Structural and operational information

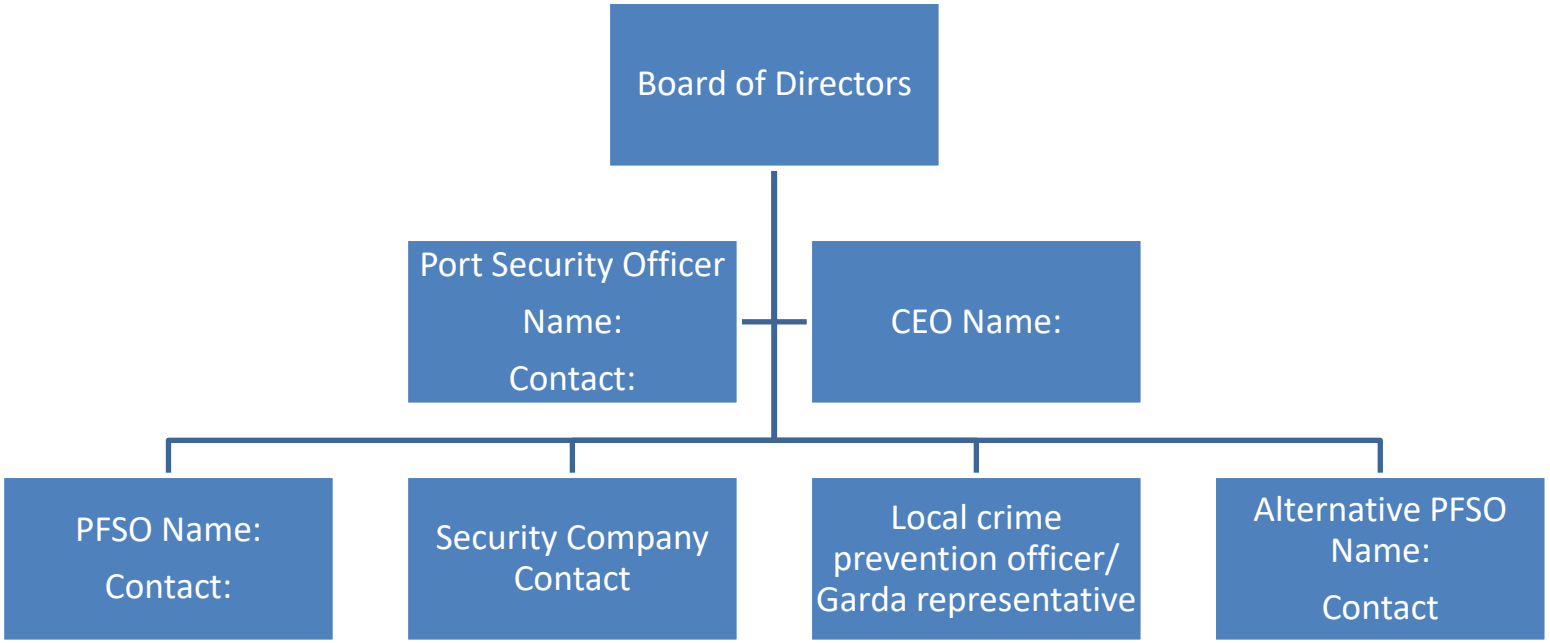
2.3 Tenants & adjacent users

Chapter 2 – 2.1 Port Facility General Information

No.	Reg 725/2004 (ISPS Code)	General Information – Port Facility	
5	-	**Name of Port Facility** Include alternate name(s)	
6	-	**Port Facility Point of Contact name(s) & phone number(s)**	
7	-	**PSO name & contact details**	
8	-	**Name & contact details of designated PFSO**	
9	-	**Is there an alternative PFSO? If Yes, give details**	Yes ☐ No☐
10	-	**Has PFSO(s) received security training, if yes, give details**	Yes ☐ No☐
11	-	**Name and contact details of local Garda Station / Crime prevention officer**	

Identify all organisational aspects relevant to port facility security

Chapter 2 –2.1 Organisational Structure



No.	Reg 725/2004 (ISPS Code)	General Information – Port Facility	
12	Part B 15.7	Size and brief description of port facility	
13	Part B 15.7	No. of Berths and vessel types (if passenger ships, state whether "turn around" facility)	
14	-	Origins & destinations of cargo shipped through port facility	
15	-	Hours of opening	
16	Part B 15.7	Does the port facility handle Dangerous Goods? If yes, give details	Yes ☐ No☐

Chapter2 – 2.2 Structural & Operational Information

No.	Reg 725/2004 (ISPS Code)	General Information – Port Facility	
17	Part B 15.7	Access Points to port facility Provide photos	
18	-	Have maps and aerial photos delineating the Ship/Shore interface boundary as per EU Regulation 725/2004 and Admiralty Charts showing adjacent water approaches to facility been provided?	Yes ☐ No☐
19	Part A 15.4	Have there been any structural or operational changes in the port facility since previous assessment?	Yes ☐ No☐ If yes, give details
20	-	Have there been any incidents recorded in the facility security log.	Yes ☐ No☐ If yes, give details

Chapter 2 – 2.3 Tenants and adjacent users

No.	Reg 725/2004 (ISPS Code)	General Information – Tenants and adjacent users	
21	Part B 15.3	Name(s) of Tenants within the facility's boundary & brief contact details (full description to be submitted in Port Facility Security Plan)	
22	Part B 15.3	Name any adjacent facilities external to the boundary and contact details (brief – full description to be submitted in Annex 1)	

Photos, Maps & Charts

Provide up to date aerial photographs, maps, drawings, plans & charts outlining, the Ship/Shore interface boundary as per EU Regulation 725/2004 and Admiralty Charts showing adjacent water approaches to facility

Chapter 3 Port Facility Security Assessment

3.1 Critical Assets

3.2 Important Assets and infrastructure

No.	Reg 725/2004 (ISPS Code)	Critical Assets – Port Facility	
23	Part A 15.5.4 & 15.5.7 Part B 15.3	Comment on structural integrity of the physical security measures e.g. fence condition, working lights, cameras etc.	
24	Part A 15.5.1 15.5.7	List cargo facilities, terminals, storage areas and cargo handling equipment	
25	Part A 15.5.1 Part B 15.3.5,.7	List systems such as electrical distribution systems, radio and telecommunication systems, computer systems and networks	

Chapter 3 – 3.1 Critical Assets

No.	Reg 725/2004 (ISPS Code)	Critical Assets	
26	Part A 15.5.1 Part B 15.3.7 15.7	List utilities, power plants, cargo transfer piping and water supplies	
27	Part A 15.5.1 Part B 15.3.6 15.7	List bridges, railways and roads infrastructure	

No.	Reg 725/2004 (ISPS Code)	Critical Assets	
28	Part A 15.5.3 Part B 15.7,15.3	List security and surveillance equipment and systems	
29		List any other operations taking place within or adjacent to port facility	
30		Identify risk variations based on seasonality/cargo	

Chapter 3 – 3.2 important assets and infrastructure

No.	Reg 725/2004 (ISPS Code)	Identification and evaluation of important assets and infrastructure which it is important to protect				
31		Prioritise list of assets and infrastructure in order of importance for protection using the following colour codes	Critical	High	Moderate	Low

Asset / Infrastructure	Operational Importance	Potential for loss of life	Economic consequences	Priority

No.	Reg 725/2004 (ISPS Code)	Identification and evaluation of important assets and infrastructure which it is important to protect				
31		Prioritise list of assets and infrastructure in order of importance for protection using the following colour codes	Critical	High	Moderate	Low

Asset / Infrastructure	Operational Importance	Potential for loss of life	Economic consequences	Priority

Chapter 4 Port Facility Risk Assessment

4.1 Risk Assessment

Chapter 4 – 4.1 Risk Assessment

Please provide a risk assessment of all critical assets at this point. A matrix format is acceptable. Your matrix should include the following:

- Threat
- Frequency of occurrence
- Probability
- Level of vulnerability
- Risk reduction measures (The score awarded to reflect the ability of the physical, electronic, human and procedural aspects of security infrastructure to the port, to actually reduce risk)

A full explanation of methodology must be provided.

The Port Facility security assessment shall include, at least the following elements:

EU Directive 725/2004 (ISPS Code Part A & B 15.5)

1. Identification of possible threats to the assets and the infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures.

   Possible acts that could threaten the security of assets and infrastructure, and the methods of carrying out those acts, should be identified to evaluate the vulnerability of a given asset or location to a security incident, and to establish and prioritise security requirements to enable planning and resource allocation. By identifying and assessing threats, those conducting the assessment do not have to rely on worst case scenarios to guide planning and resource allocations.

The PFSA should consider all possible threats, which may include the following types of security incidents:

- Damage to, or destruction of the port facility or of the ship e.g. by explosive devices, arson, sabotage or vandalism
- Hijacking or seizure of the ship or of persons on board
- Tampering with cargo, essential ship equipment or systems or ship's stores
- Unauthorised access or use including presence of stowaways
- Smuggling weapons or equipment, including weapons of mass destruction
- Use of the ship to carry those intending to cause a security incident and their equipment
- Use of the ship itself as a weapon or as a means to cause damage or destruction
- Blockage of port facility entrances, locks approaches etc.
- Nuclear, biological and chemical attack
- Possibility of cluster effects of security incident
- Unauthorised UAV activity

2. Identification, guidance, selection and prioritisation of counter measures and procedural changes and their level of effectiveness in reducing vulnerability; and

3. Identification of weaknesses, including human factors in the infrastructure, policies and procedures.

   Identification of vulnerabilities in physical structures, personnel protection systems, processes or other areas that may lead to a security incident can be used to establish options to eliminate or mitigate those vulnerabilities. For example, an analysis might reveal vulnerabilities in a port facility's security system or unprotected infrastructure such as water supplies, bridges etc. that could be resolved through physical measures e.g. permanent barriers, alarms surveillance equipment etc.

   Identification of vulnerabilities should include consideration of:

   - Waterside and shore side access to the port facility and ships 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 port facility services and utilities
   - Measures to protect radio and telecommunication equipment, port facility services and utilities, including computer systems and networks including cyber security measures
   - Adjacent areas that may be exploited during or for an attack
   - Existing agreements with private security companies providing waterside/shore side security services
   - Any conflicting policies between safety and security measures and procedures
   - Any conflicting port facility and security duty assignments
   - Any enforcement and personnel constraints
   - Any deficiencies identified during training and drills
   - Any deficiencies identified during daily operation, following incidents and alerts, the report of security concerns, the exercise of control measures, audits etc.

*Refer to Waterside Assessment

RSO Report of PFSA

A report by the RSO is required. See Chapter 7.

Chapter 5 Current Port Facility Security Measures

5.1 Structural Port Facility Security

5.2 Procedural Port Facility Security

No.	Reg 725/2004 (ISPS Code)	5.1 Structural Security Measures	
32	Part A 15.5.4 Part B 15.3.8	List any areas which if damaged or used for illicit observation, may pose a risk to persons, property or operations within the port facility. (Consider UAV risk)	
33	Part A 15.5.3 Part B 15.13 15.14.4	Brief details of any passenger or vehicle security arrangements (e.g. boarding cards, restricted areas, screening, searching, unaccompanied baggage etc.)	
34	Part B 15.3.4	Outline security clearance standards, specifically "need to know" requirements of those directly involved	
35	Part B 15.4	Brief details of cargo handling security arrangements including cranes, straddle carriers, tugs etc.	

Chapter 5 – 5.1 Structural Port Facility Security Measures

No.	Reg 725/2004 (ISPS Code)	Structural Security Measures	
36	Part A 15.5 Part B 15.3.1 15.3.2	Identify all security infrastructure including: Fences, Access gates, Entry control points, High level lighting, CCTV cameras (fixed, tilt, IR etc.), continuous monitoring or recorded. Comment on the structural integrity of the physical security measures	
37	Part A 15.5 Part B 15.3.1, .2	Identify CCTV storage locations	
38	-	Period of time footage is stored	
39	Part A 15.5	Comment on the protection of communications hub	

	Part B 15.3.1, .2		

Chapter 5 – 5.2 Procedural Port Facility Security Measures

No.	Reg 725/2004 (ISPS Code)	Procedural Security Measures	
40	**-**	**Is there an approved Port Facility Security Assessment as per Regulation 725/2004**	Yes ☐ No☐
41	**-**	**Is there an approved Port Facility Security Plan.** **If Yes, where is it stored and what personnel have access?**	Yes ☐ No☐
42	**Part A 15.5.3** **Part B 15.16**	**Brief details of any existing arrangements with private security companies.**	

43	**Part A 15.5.3** **Part B 15.16**	**Is the security company PSA approved?**	Yes ☐ No☐

No.	**Reg 725/2004 (ISPS Code)**	**Procedural Security Measures**	
44	**Part B 15.3.3**	**List personnel security systems (e.g. clearance, ID, alarms, types of passes)**	
45	**Part B 15.3.3**	**Identify which port facility personnel will be subject to background checks / security vetting. NB. Consider not only external threats to the security of the port but also internal threats to security**	

46	**Part B 15.3.3** **Part B 15.16.10**	**How often is personnel security pass system audited?**	
47	**Part B 15.3.3**	**Is there an out of hours security patrol? If yes, give details**	Yes ☐ No☐

No.	**Reg 725/2004 (ISPS Code)**	**Procedural Security Measures**	
48	**Part A 15.5**	**Provide list of restricted areas within the Port Facility**	
49	**-**	**Provide list of assembly points**	
50	**Part A 15.5.3**	**List available security staff & additional equipment provision in the event of Level 2 or Level 3 security incidents**	

51	**Part B 15.3.4**	**Detailed maritime security training to facility staff and contractors**	
52	**Part B 15.14**	**Is there a system of maritime security drills, exercise & auditing in place? Details**	Yes ☐ No☐

No.	**Reg 725/2004 (ISPS Code)**	**Procedural Security Measures**	
53	**Part A 15.4** **Part B 15.3.4**	**Procedures for adapting and updating the port facility security assessment and plan**	
54	**Part B 15.3.4**	**Procedures for protecting sensitive and restricted information either electronically or in paper form**	

55	**Part B 15.3.4**	**Identify how measures, procedures and actions will be reinforced in the event of an increase in security level**	
56	**Part A 15.4.3** **Part B 15.3.4, .13** **Part B 15.16**	**Specific requirements for dealing with established security concerns such as suspect cargo, luggage, bunker, provisions or persons unknown parcels, known dangers (bombs)**	
57		**Has the Port Facility taken into account the IMO GUIDELINES ON MARITIME CYBER RISK MANAGEMENT, See** MSC-FAL.1-Circ.3-Rev.2 – Guidelines On Maritime Cyber Risk Management (Secretariat) (1).pdf (imo.org) **& EU Guidance on how to treat cybersecurity at the port facility and port level (see Annex 3)?**	
58		**Are measures in place for protecting electronic operational systems, security pass systems, records etc.**	
59		**Are port facility staff trained in cyber security awareness?**	

No.	Reg 725/2004 (ISPS Code)	Identify measures at **Security Level 1** encompassing Regulation 725/2004 (the level for which minimum appropriate security will be maintained at all times) ***Ensure the information provided is concise and factual.***	**List deficiencies and breeches in respect of each measure.**
60	**Part B** **15.16.3** **15.16.4** **15.16.12**		

No.	Reg 725/2004 (ISPS Code)	**Identify additional measures at Security Level 2 encompassing Regulation 725/2004** (the level for which additional security measures shall be maintained for a period of time as a result of heightened risk) ***Ensure the information provided is concise and factual.***	
61	**Part B** **15.16.3** **15.16.4** **15.16.12**		

No.	Reg 725/2004 (ISPS Code)	**Identify further additional measures at Security Level 3 encompassing Regulation 725/2004** (the level for which further specific measures shall be maintained for a limited period of time when a security incident is probable or imminent although it may not be possible to identify the specific target) ***Ensure the information provided is concise and factual.***	**List deficiencies and breeches in respect of each measure.**
62	**Part B** **15.16.3** **15.16.4** **15.16.12**		

Chapter 6 Port Facility Waterside Assessment

6.1 Overview

6.2 General Information

6.3 Assets & infrastructure

Overview

The waterside assessment should cover all waterside access extending from approaches, channels and anchorages, up to and including each facilities ship/shore access, details of all relevant assets including vessel traffic monitoring hubs.

A risk analysis should be included in your water assessment, identifying threats, frequency, probability, level of vulnerability and risk reduction measures.

A matrix format is acceptable, a full explanation of methodology must be provided.

Chapter 6 – 6.2 Waterside General Information

No.	Reg 725/2004 (ISPS Code)	Waterside Assessment General Information	
63	Part B 15.16.1 15.7.9	Provide a brief description of the overall area involved	
64	Part B 15.16.1 15.7.9	List anchorages, channels, manoeuvring & berthing areas	
65	Part B 15.16.1 15.7.9	Brief description of individual berths and adjacent water approaches. Provide photos	

No.	Reg 725/2004 (ISPS Code)	Waterside Assessment General Information	
66	Part B 15.16.1 15.7.9	List Port vessel traffic management systems & aids to navigation relevant to the port facility	
67	Part B 15.16.1 15.7.9	List port facility service vessels including pilot boats, tugs & lighters etc.	

Chapter 6 – 6.3 Waterside assets & infrastructure

No.	Reg 725/2004 (ISPS Code)	Identification and evaluation of important assets and infrastructure which it is important to protect				
68		Prioritise list of assets and infrastructure in order of importance for protection using the following colour codes	Critical	High	Moderate	Low

Asset / Infrastructure	Operational Importance	Potential for loss of life	Economic consequences	Priority

No.	Reg 725/2004 (ISPS Code)	Identification and evaluation of important assets and infrastructure which it is important to protect				
69		Prioritise list of assets and infrastructure in order of importance for protection using the following colour codes	Critical	High	Moderate	Low

Asset / Infrastructure	Operational Importance	Potential for loss of life	Economic consequences	Priority

Waterside Risk Analysis

Please provide a risk analysis identifying threats, frequency, probability, level of vulnerability and risk reduction measures.

A matrix format is acceptable, a full explanation of methodology must be provided.

Maps, Photos & charts of water approaches, berths, anchorages and manoeuvring areas.

Chapter 7 Report of RSO and Identification of Vulnerabilities & Recommendations

Upon completion of the port facility security assessment, a report shall be prepared by the RSO. This report shall comprise the following

- A summary of how the assessment was conducted (This may be inserted below or may be annexed to the PFSA document at Annex 2)
- A description of each vulnerability found during the assessment (to be included below)
- A description of countermeasures that could be used to address each vulnerability (to be included below)

Identification of vulnerabilities & Recommendations		
No	**Area/Topic – Description of Vulnerability**	**Description of countermeasures to address vulnerability**

Identification of vulnerabilities & Recommendations		
No	**Area/Topic – Description of Vulnerability**	**Description of countermeasures to address vulnerability**

Checklist

Name of Port Facility:			**Date:**		**Issue Number:**
Port Facility Security Plan	☐	Security personnel	☐	Physical security	☐
Communications systems	☐	Lighting	☐	Navigation systems	☐
Port facility operations	☐	Infrastructure and services	☐	Passenger vessels (types of operations)	☐
Intruder alarm systems	☐	Designated port facility area	☐	Passengers – boarding cards, area checks and searches.	☐
CCTV systems	☐	Restricted areas	☐	Passenger vehicles	☐
Access control systems	☐	Water approaches and patrols	☐	Luggage	☐
Security patrols and manning	☐	Access to ships	☐	Stores	☐
Security awareness training	☐	Port facility personnel procedures	☐	Security levels 2 & 3	☐
Security organisation and Management	☐	Ship personnel	☐	Crew change	☐
Berths	☐	Cargo	☐	Cyber Security Measures	☐
UAV's (Drones) measures	☐				
Document Check list					
Drawings of port facility boundary	☐	Lighting footprint	☐	CCTV locations	☐
Aerial photos delineating facility boundary	☐	Photos of access points	☐	Critical infrastructure	☐
Ship/Shore interface	☐	Photos of restricted areas	☐	Photos of fencing	☐
Appended Adjacent users & Tenants list	☐	Water assessment, charts, maps & photos	☐		

Annex

1. **List of Tenants and adjacent users**
2. **Report of RSO**
3. **Guidance on how to treat cybersecurity at the port facility and port level**

1. Annex 1. List of Tenants and adjacent users

No.	Organisation Name	Involved in Maritime Transport	Business Type	Tenant Security Measures					Direct contacts	
				Alarm	Fence	CCTV	Security Contract	Security Procedures	Contact Name	Phone Number

No.	Organisation Name	Involved in Maritime Transport	Business Type	Tenant Security Measures					Direct contacts	
				Alarm	Fence	CCTV	Security Contract	Security Procedures	Contact Name	Phone Number

2. Annex 2. Report of RSO. (See Ch. 7)

Insert / attach report of RSO.

3. Annex 3

Guidance on how to treat cybersecurity at the port facility and port level

Background

The European Commission presented a draft of this guidance to Member States in the Workshop on Cybersecurity in the Maritime Sector of 8 November 2022. Following feedback received, this guidance is presented to the 89th meeting of the Committee for Maritime Security.

Introduction

The European Commission has found it useful to propose the development of this guidance document to clarify the legislative requirements concerning the security of network and information systems used by ports and port facilities, according to Regulation (EC) No 725/2004 of 31 March 2004 on enhancing ship and port facility security and Directive 2005/65/EC of 26 October 2005 on enhancing port security.

The document also offers a non-exhaustive set of guidance that may apply, in particular if a Port Facility Security Assessment (PFSA) has found vulnerabilities[1] relating to cybersecurity. It does not change any legal requirements. The European Commission notes that guidance material already exists on cybersecurity in the maritime sector, but that this document aims to focus on those security measures and mechanisms that are defined in the existing EU maritime security legislation.

The European Commission also notes that this EU maritime security legislation is focused on physical security, but nevertheless provides a useful framework through which to consider where cybersecurity risk-management measures may be the most useful, for example when it comes to

[1] When referring to "vulnerabilities" in the context of this guidance document, there is a focus on the vulnerabilities to incidents that could impede the operational functioning of the port facility or affect the security of persons, as understood under Regulation 725/2004 – this is a more narrow focus than what is defined as a "vulnerability" in the NIS 2 Directive (see page 3)

access control and cargo handling. Some ports may already be concerned by the cybersecurity requirements put in place by the NIS Directive[2] and the subsequent NIS 2 Directive[3].

This guidance also aims to address how requirements from EU maritime security legislation and the NIS and NIS 2 Directives may be considered together and how they may complement each other. With regard to the entities falling under the scope of the NIS 2 Directive, this guidance is without prejudice to the cybersecurity risk-management and reporting requirements under the NIS 2 Directive, including as elaborated in the implementing acts to be developed pursuant to its Articles 21 and 23.

The maritime sector increasingly uses digital technologies[4], which brings many benefits but also certain risks to cyber-incidents. Security systems themselves in port facilities and ports may increasingly rely on digital technologies. The European Commission hopes that this document will assist Member States and port facilities/ports to take on challenges relating to cybersecurity.

Legislative requirements

[2] Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (to be repealed by the NIS 2 Directive with effect from 18.10.2024)

[3] Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[4] When referring to “digital technologies” or “systems” here, we mean what is described as “computer systems and networks” in Regulation 725/2004, and as “network and information systems” in the NIS/ NIS 2 Directive

Regulation 725/2004

Annex III, Paragraph 15.3.5

"*A PFSA should address the following elements within a port facility: […] radio and telecommunication systems, including computer systems and networks*"

- This means that a PFSA must consider the security of computer systems and networks
- As a result of this, the resulting port facility security plan (PFSP) must develop measures to address the vulnerabilities concerning computer systems and networks identified in the PFSA[5], if any have been found
- European Commission inspections may then verify the above, as the minimum needed to be in conformity with the legislation

Beyond this, the below guidance develops on how to treat cybersecurity in port facilities and ports through the EU maritime security legislation in place.

Guidance for port facilities

Regulation 725/2004

Port facility security assessment

[5] Regulation 725/2004, Annex II, Paragraph 16.1

One of the most straightforward ways of satisfying the requirement of Annex III Paragraph 15.3.5 of Regulation 725/2004 is to include a cybersecurity threat scenario in the PFSA, in the risk analysis of vulnerabilities. There may be several scenarios, which may go into varying levels of detail, depending on the situation of each port facility.

To carry out this assessment, those involved in preparing the PFSA should be able to liaise with personnel responsible for the cybersecurity of the port facility. If such a task is not assigned to specific staff, they should draw on the expertise of cybersecurity experts. This is in line with Annex III Paragraph 15.4.11 of Regulation 725/2004.

In considering cybersecurity in the PFSA, the primary concern must remain the avoidance of death or injury[6]. The PFSA may then consider cyber attacks used in conjunction with physical attacks (hybrid attacks), and so may focus on aspects such as how security systems and equipment, or access control, can be vulnerable to cyber attacks.

It is also important to consider assets which are key to the operational functioning of the port facility[7] and how they could be vulnerable to cyber attacks, for example digital cargo manifests used for handling cargo, or digital card readers for access control. In this sense, considering threat scenarios that focus on the relation between IT and OT systems is recommended. Higher reliance on IT and OT systems should entail stricter cybersecurity measures.

It is important to highlight that when referring to “vulnerabilities” in the context of this guidance document, there is a focus on the vulnerabilities to incidents that could impede the operational functioning of the port facility or affect the security of persons, as understood under Regulation

[6] Regulation 725/2004, Annex III, Paragraph 15.6
[7] ibid

725/2004. This is a more narrow focus than what is defined as a "vulnerability" in the NIS 2 Directive, which is "a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat"[8].

In the same way, this guidance document may refer to "cyber attacks" instead of "cyber incidents". Regulation 725/2004 was designed to protect shipping and port facilities against threats of intentional unlawful acts, meaning deliberate acts which could cause harm[9]. An "incident" under the NIS 2 Directive has a wider meaning and may concern incidents that are not deliberate cyber attacks[10]. It is to be noted that there are examples of cyber incidents which were deliberate but not targeted, in particular the NotPetya attack affecting Maersk in 2017.

Maritime cybersecurity threats[11] should then be considered and treated as any other maritime security threat in the PFSA, along the same 4-step approach described in Regulation 725/2004, Annex II, Paragraph 15.5.

The ENISA Guidelines on "Cyber Risk Management for Ports" and the related online tool are useful resources when assessing cybersecurity risks in a port facility or port[12].

[8] Directive 2022/2555, Article 6 (15)
[9] Regulation 724/2004, Article 2 (13)
[10] See Directive 2022/2555, Article 6 (6)
[11] "Cyber threats" are defined in the Cybersecurity Act (Regulation (EU) 2019/881) as any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons
[12] See internet links: Guidelines - Cyber Risk Management for Ports — ENISA (europa.eu) and Cyber risk management for ports — ENISA (europa.eu)

Port facility security plan

The PFSP must develop measures to address the vulnerabilities concerning computer systems and networks identified in the PFSA, if any have been found. These must include procedures for addressing cyber threats or responding to cyber attacks including provisions for maintaining critical operations of the port facility or ship/port interface[13].

Based then on the results of the PFSA, there may be several aspects that the PFSP should address when considering cybersecurity[14], and which are described below.

Security organisation of the port facility[15]

The PFSP should describe the roles and responsibilities of cyber security personnel for the facility, including how and when physical security and ICT security personnel will coordinate activities and conduct notifications for suspicious activity, breaches of security, or heightened security levels. This could concern in particular, for example, the figure of the Chief Information Security Officer (CISO).

[13] Regulation 725/2004, Annex II, Paragraph 16.1
[14] Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) defines "cybersecurity" as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats"
[15] Regulation 725/2004, Annex III, Paragraph 16.3.1

Links with other authorities[16]

The PFSP should detail the port facility's links with other relevant authorities, in particular here, cybersecurity authorities (e.g. national cybersecurity authority or computer security incident response teams designated under the NIS/NIS 2 Directive) that it may need to contact in case of a cyber incident, threat or suspicious activity.

Communication systems

The PFSP must detail the necessary communication systems to allow the effective continuous operation of the organisation and its links with others, including ships in port[17].

To the extent that ICT systems are used to perform this function, the PFSP should describe how those systems are protected, an approved and secure alternative means of communication, and the personnel communication responsibilities should the system be compromised or degraded.

Security levels

[16] Regulation 725/2004, Annex III, Paragraph 16.3.2
[17] ibid

The PFSP should detail if additional cybersecurity measures are to be put in place at security level 2 and/or 3[18]. For example, additional readiness to switch from digital to paper-based operations, without external electricity or with limited internet/mobile network connections. Another example is to verify that the database on the persons with permission to access the port facility had not been altered.

Reporting security incidents

The PFSP may detail the procedures for reporting a cybersecurity incident[19].

There are relevant provisions here in the NIS 2 Directive. The concerned entity must notify the NIS competent authority or the computer security incident response team (CSIRT) designated under the NIS/NIS 2 Directive any significant incident[20]. Port facilities which do not fall under the scope of the NIS 2 Directive may voluntarily report incidents, cyber threat and near misses to the same entities[21].

[18] Regulation 725/2004, Annex III, Paragraph 16.3.4
[19] Regulation 725/2004, Annex II, Paragraph 16.3.9
[20] Directive 2022/2555, Article 23 (1)
[21] Directive 2022/2555, Article 30

According to Regulation 725/2004, a "security incident" means any suspicious act or circumstance threatening security, of a port facility in this case[22]. In the NIS 2 Directive, an "incident" means "an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems"[23].

In the context of port facility security under Regulation 725/2004, a "cybersecurity incident" that should be reported is an incident that compromises the functioning of operations in the port facility (including ship/port interface), such as cargo handling equipment or digital cargo manifests. In particular, if this can have an impact on the security of persons, for example operational technology used for access control. Failed or countered cyber attacks (near misses[24]) that would otherwise have had such consequences should also be reported.

If a cybersecurity incident is reported to a national authority competent for cybersecurity, the national authority competent for maritime security should also be informed, either by the port itself or by the cybersecurity national authority, depending on how the Member State wishes to organise this. The opposite should also apply: if a cybersecurity incident is reported to a maritime authority, then the national authority competent for cybersecurity, the CSIRT or SPOC designated under the NIS/NIS2 Directive should also be informed.

In general, close cooperation between the responsible maritime and cybersecurity authorities in a Member State is strongly encouraged as regards port cybersecurity. It should be noted that in some Member States the authorities competent for port security and port cybersecurity are the same, which then facilitates coordination.

Records of cybersecurity incidents should be kept.

It is also recommended that a root cause analysis is carried out following a cybersecurity incident by the PFSO and their cybersecurity experts, in order to more systematically prevent and solve underlying issues. As a reminder, a PFSP must be reviewed or audited in response to experience

[22] Regulation 725/2004, Annex I, Regulation 1, Paragraph 1.13
[23] Directive 2022/2555, Article 6 (6)
[24] See definition in Directive 2022/2555, Article 6 (5)

or changing circumstances[25]. A successful cyber attack should be understood as such an experience or changing circumstance. A PFSA must also be periodically reviewed and updated, taking account of changing threats[26].

Information sharing of anonymised data with relevant entities, such as information sharing and analysis centres, is encouraged in order to raise awareness and increase capacity building within the broader maritime transport sector.

Drills and exercises

As drills should test individual elements of the PFSP[27], if cybersecurity measures are included in the PFSP, then some drills may focus on readiness against cyber attacks and the personnel's knowledge of cybersecurity.

This could include, for example, sending a "fake" phishing email to all staff.

In the same way, an exercise may test a scenario involving or focused on a cyber attack. For example, a "red-team" exercise can promote technical, organisational and human interactions.

Having said this, the quarterly drills and yearly exercises should not become overwhelmingly devoted to cybersecurity. As usual, drills and exercises are meant to test the security readiness in the face of the diversity of threats identified by the PFSP.

As usual, records of drills and exercises should be kept.

[25] Regulation 725/2004, Annex III, Paragraph 16.3.5
[26] Regulation 725/2004, Annex II, Paragraph 15.4
[27] Regulation 725/2004, Annex III, Paragraph 18.5

Training

In order to understand the cybersecurity provisions that are included in the PFSP (if this is the case), the PFSO should have a baseline knowledge of cybersecurity concepts and attack scenarios. This guidance document, the DG MOVE Transport Cybersecurity Toolkit[28] and the ENISA Guidelines on "Cyber Risk Management for Ports" can be useful tools in this regard. The PFSO should also know the emergency preparedness and response and contingency planning[29] in case of a cyber attack, for example which national authority to contact in case of a cyber attack.

In the same way, port facility personnel with specific security duties should have knowledge of cybersecurity threats[30], in particular those most relevant to their port facility. Port facility personnel having specific duties in cybersecurity in turn should have knowledge of the security organisation of the port facility, in particular where a need for coordination with physical security personnel has been identified.

It is also encouraged that all port facility personnel have some basic cybersecurity knowledge, to create a cybersecurity culture across the organisation, particularly on phishing emails and social engineering, whereby the human factor is more relevant.

The PFSP should describe the cybersecurity training requirements put in place of port facility personnel with a security role, if such is the case[31].

[28] See internet link: Cybersecurity (europa.eu)
[29] Regulation 725/2004, Annex III, Paragraph 18.1.9
[30] Regulation 725/2004, Annex III, Paragraph 18.2.1
[31] Regulation 725/2004, Annex III, Paragraph 16.8.2

Documentation and records

Electronic records should be protected against unauthorized deletion, destruction, or amendment. In this regard, the PFSP must establish the procedures and practices to protect security-sensitive information held in electronic format[32].

In addition, the PFSO should liaise with cybersecurity personnel to define digital file access privileges to sensitive data or functions within the network.

If the PFSP is kept in electronic format, then it must be protected by procedures aimed at preventing its unauthorised deletion, destruction or amendment[33].

Security systems and equipment maintenance

The PFSP should describe or refer to cyber-related procedures for managing software updates and patch installations on systems used to perform or support functions identified in the PFSP (e.g. identification of needed security updates, planning and testing of patch installations).

Access control

[32] Regulation 725/2004, Annex III, Paragraph 16.8.6
[33] Regulation 725/2004, Annex II, Paragraph 16.7

The PFSP should identify digital systems that control physical access devices such as gates and cameras, as well as digital systems within secure or restricted areas, such as cargo or industrial control systems. It may also include specific minimum security requirements, such as multi-factor authentication and digital access management.

Restricted areas

When describing restricted areas, the PFSP should take into account how digital systems may control authorised access to those restricted areas. For example, unauthorised access might be possible by manipulating a digitally controlled gate, allowing physical access, or by accessing the protected system via cyber means, such as by hacking into files that contain sensitive security information relating to restricted areas.

Areas containing sensitive OT or IT control components (e.g. server rooms, routers, modems) may themselves be defined as restricted areas.

Port facility operations

The PFSP should include cybersecurity measures that protect the handling of electronic files and documentation which are used in common port facility operations such as cargo handling and delivery of stores. For example, cargo manifests and other cargo documentation should be protected, to deter tampering, prevent unauthorised loading/unloading of cargo, and prevent acceptance of cargo that is not meant for carriage.

Audits

The port facility may choose to conduct the cybersecurity portion of their audits with either the aid of cyber security specialists from a third party or within the organisation. The audit report should clearly indicate that the cybersecurity provisions detailed in the PFSP are in place and are considered to be appropriate and effective. The audit should include the name, position, and qualification of the person conducting the audit.

Guidance for ports

Directive 2005/65/EC

Port security assessment and Port security plan

Article 4 of the Directive states that port security measures should be closely coordinated with measures taken pursuant to Regulation 725/2004. So if cybersecurity has been assessed as an important aspect for one or several port facilities of a port, then this should be reflected in the port security assessment and plan.

The PSA may include a threat scenario of a cyber incident concerning the whole or an important part of the port, or several threat scenarios. The extent and detail of these scenarios may depend on the complexity of the unique environment of each port.

Cybersecurity personnel may be included among the port personnel that must be subject to background checks and/or security vetting.

The port may be subdivided according to the likelihood and impact of cybersecurity incidents.

When identifying all organisational aspects relating to port security, authority over the cybersecurity of the port should be taken into account.

Cybersecurity incidents should be included among the clear reporting requirements to the port security officer and/or to the port security authority.

Cybersecurity plan

If cybersecurity procedures for the port have been set out in a separate plan, such as a plan related to the compliance with the requirements of the NIS/ NIS 2 Directive, then the PSP must detail interaction and coordination with this cybersecurity plan. Where necessary conflicts and shortcomings must be resolved[34].

It is also possible to annex the cybersecurity plan to the PSP, keeping in mind the appropriate level of classification.

If the cybersecurity provisions in a separate plan are directly relevant to measures that should be put in place in the context of EU maritime security legislation, for example the protection of cargo handling operations, then appropriate reference should be made in the relevant PFSP or PSP. EU Commission inspections may then verify these provisions in the cybersecurity plan.

Training exercises

Exercises concerning a cybersecurity threat scenario may be considered as an exercise satisfying the requirements of Annex III of the Directive, if cybersecurity is identified as a threat under the PSA.

Conclusion

[34] Directive 2005/65, Annex II

With cybersecurity increasingly being a challenge for the maritime sector, and in particular ports, the European Commission wishes to clarify the relevant provisions of EU maritime security legislation in this regard, through this guidance document. As maritime and cybersecurity practices evolve with time, this guidance may be updated.