Port Security Assessment 2024 - 2029

Port Security Assessment pursuant to the European Communities (Port Security) Regulations 2007 (Directive 2005/65/EC of the European Parliament).

Port Name:

Port Security Assessment 2024 – 2029 (PSO 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 9
Review 9
Glossary & Definitions 10
Chapter 1 General Information 11
Chapter 1- 1.1 Assessment Team 12
Chapter 2 Port General Information 13
Chapter 2 – 2.1 Port General Information 14
Chapter 2 –2.1 Organisational Structure 15
Chapter2 – 2.2 Structural & Operational Information 17
Chapter 2 – 2.4 Port Boundary 19
Chapter 3 Port Security Assessment 21
Chapter 3 – 3.1 Critical Assets 22
Chapter 3 – 3.1 Critical Assets 23
Chapter 3 – 3.1 Critical Assets 24
Chapter 3 – 3.2 Identification and evaluation of important assets and infrastructure which it is important to protect 25
Chapter 4 Port Risk Assessment 27
Chapter 4 – 4.1 Risk Assessment 28
Chapter 5 Current Port Security Measures 31

Chapter 5 – 5.1 Structural Port Security Measures 32
Chapter 5 – 5.1 Structural Port Security Measures 33
Chapter 5 – 5.2 Procedural Port Security Measures 34
Chapter 5 – 5.2 Procedural Port Security Measures 35
Chapter 5 – 5.2 Procedural Port Security Measures 36
Chapter 6 Port Waterside Assessment 43
Overview 44
Chapter 6 – 6.2 Waterside General Information 45
Chapter 6 – 6.3 Waterside assets & infrastructure 47
Waterside Risk Analysis 48
Maps, Photos & charts of water approaches, berths, anchorages and manoeuvring areas. 50
Chapter 7 Identification of Vulnerabilities & Recommendations 51
Checklist 53
Annex 54
Annex 1. List of Tenants and adjacent users 55
Annex 2. Guidelines for the definition of port boundaries 57
Annex 3. Guidance on how to treat cybersecurity at the port facility and port level 68

Overview & Background

For the information of Ports,Tenants and users, owners or operators of adjacent infrastructure and Recognised Security Organisations (Ports).

(Please refer to: EU Directive 2005/65/EC, ISPS Code 2004, SOLAS Chapter XI-2, Regulation 10, Irish S.I 413/2004 EC & Port Facility Regulations, and S.I. 284/2007 EC Port Security 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 maritime security measures imposed by that Regulation constitute only part of the measures necessary to achieve an adequate level of security throughout maritime-linked transport chains. That Regulation is limited in scope to security measures on board vessels ***and the immediate ship/port interface.***

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 Members 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.
The Regulation & Directive arrangements in ports are subject to a five year review and for the next period between 2024 - 2029, compliance by all ports and port facilities is due by July 1st 2024

Prior to 2014, port facilities were required to undertake separately both a Port Security Assessment and a Port Facility Security Assessment, resulting in a significant duplication of work. For the 2014 – 2019 period, a "combined assessment" was completed for each port facility. Following inspections in Ireland by the European Commission in 2015 and 2018, it was necessary to further modify the assessment methodology as below:

- A single port security assessment (this template) is required to be completed to cover all areas of the port and this is to be submitted in SSI by the Port Security Officer for approval by the Marine Survey Office. (to be uploaded in SSI under the page for the designated "main" port facility of the port as agreed with the MSO). Each port is responsible for undertaking its own port security assessment, using an approved Recognized Security Organization (RSO) (Ports). Whereas the full co-operation of tenants, owners and operators of facilities, infrastructure, or properties within the port area is expected in relation to the carrying out of a port security assessment, Regulation 12(c) of the European Communities (Port Security) Regulations 2007 provides for the unlikely circumstance where this activity is obstructed or impeded and the MSO should be contacted accordingly:

12. (1) A person who obstructs or impedes—

(*a*) an authorised officer in carrying out a conformity check under Regulation 11,

(*b*) the implementation of a port security plan or any action or training exercise taken in relation to it, or

(*c*) a recognised security organisations in carrying out a port security assessment,

commits an offence.

- Each port facility (including the "main" PF mentioned above) will also be required to have a port facility security assessment. (see separate PFSA template) and this is to be submitted in SSI by the Port Facility Security Officer for approval by the Marine Survey Office. Each port facility is responsible for undertaking its own port facility security assessment, using an approved RSO (Ports).

Port Boundary

The definition of the port boundary has also been raised by the EC during their inspection activity in Ireland . The European Commission considers that the TAPS II study[1] which identifies the various parameters affecting the definition of the port boundaries and develops a methodology based on a systemic process for the definition of the port boundary should be taken into account.

In carrying out the Port Security Assessment, the RSO (Port) in consultation with the Port Security Officer must identify the port boundary taking into account the TAPs II approach. The MSO will not consider approval of a port boundary unless this approach has been undertaken.

The TAPs II process consists of two fundamental checks / controls:

- the first is aimed at defining which port facilities and essential port elements are to be considered parts of the same port, and,
- the second is aimed specifically at defining effective port security boundaries after a comprehensive security risk analysis.

The proposed methodology addresses the following steps:

- Identification of port essential elements
- Definition of the reference boundaries
- Verification of the port layout and clusters of port areas
- Identification of crossed vulnerabilities
- Identification and verification of port security boundaries

The port security assessment must also address the following:

- identification and evaluation of important assets and infrastructure which it is important to protect;
- identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures; (including taking account of cyber security issues (see Annex 3) and the incursion of Unmanned Aerial Vehicles UAV's / Drones etc.)

[1] See Annex 2 - Guidelines for the definition of port boundaries under Directive 2005/65/EC on enhancing port security and TAPs II methodology

- 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
- identification of all areas which are relevant to port security

Port Security Assessment General

The Port Security Assessment will comprise of both a landside and waterside assessment of the port, (refer to TAPS II document for guidance) and will include a risk assessment of all areas to establish potential threats (including cyber threats) to the port.

Waterside assessment modules should be arranged by the PSO of the Port and involve the Harbour Master or other competent personnel.

All completed or amended port security assessments must be uploaded onto the Safe Seas Ireland (SSI) network.
Comments/approvals of port security assessments by the Administration will be posted via the SSI network.

When carrying out port security assessments, RSO's and PSO's should also take account of Section 8 of the European Commission MARSEC Doc. 9108 annex -Interim Guidance on Maritime Security for Member States' Competent Authorities.

Brian Hogan
Chief Surveyor
Irish Maritime Administration

Scope

This template will be used to assess the security of all ports as designated by the Administration. [2]

Review

Member States have to ensure that port security assessments and port security plans are reviewed as appropriate. They shall be reviewed at least once every five years. Port companies are obliged to resubmit Port Security Assessments in the event of any operational or procedural changes to a port or 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.

[2]Not required for ports receiving no more than 12 “ISPS” ship arrivals per year.

Glossary & Definitions

Port: means any specified area of land, with boundaries defined by the Minister under Regulation 3 of the European Communities (Port Security) Regulations 2007, in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport .

Port Boundary: the "virtual" security boundary around a port to include not just the entire operational and legal boundary of the port, but also any adjacent areas, buildings, infrastructure or operations which might have a negative impact on port operation, should a security incident occur involving such areas, buildings, operations or infrastructure.[3]

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 Authority: means the authority responsible for security matters in a given port as designated by the Minister. A Port Security Authority is required for each port.[2] A Port Security Authority may be designated for more than one port.

Port Security Officer (PSO): A Port Security Officer shall be approved by the Marine Survey office 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 Security Assessment: Each port security assessment shall be carried out taking into account as a minimum the detailed requirements laid down in Annex I of Directive 2005/65/EC. Port security assessments may be carried out by a recognised security organisation (ports). Port security assessments shall be approved by the Marine Survey Office.

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

[3] See Annex 2 - Guidelines for the definition of port boundaries under Directive 2005/65/EC on enhancing port security and TAPs II methodology

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.	EU Directive	General Information – Assessment Team	
1		**Date of Assessment / Survey**	
2		**Name(s) of person(s) carrying out assessment**	
3	**Annex I**	**Relevant skills and expertise of assessors.**	
4		**Consultation with national Authorities relating to potential threats to port**	Yes ☐ No☐ Give details

Chapter 2 Port General Information

2.1 General Information & Organisational Structure

2.2 Port Structural and operational information

2.3 Tenants & adjacent users

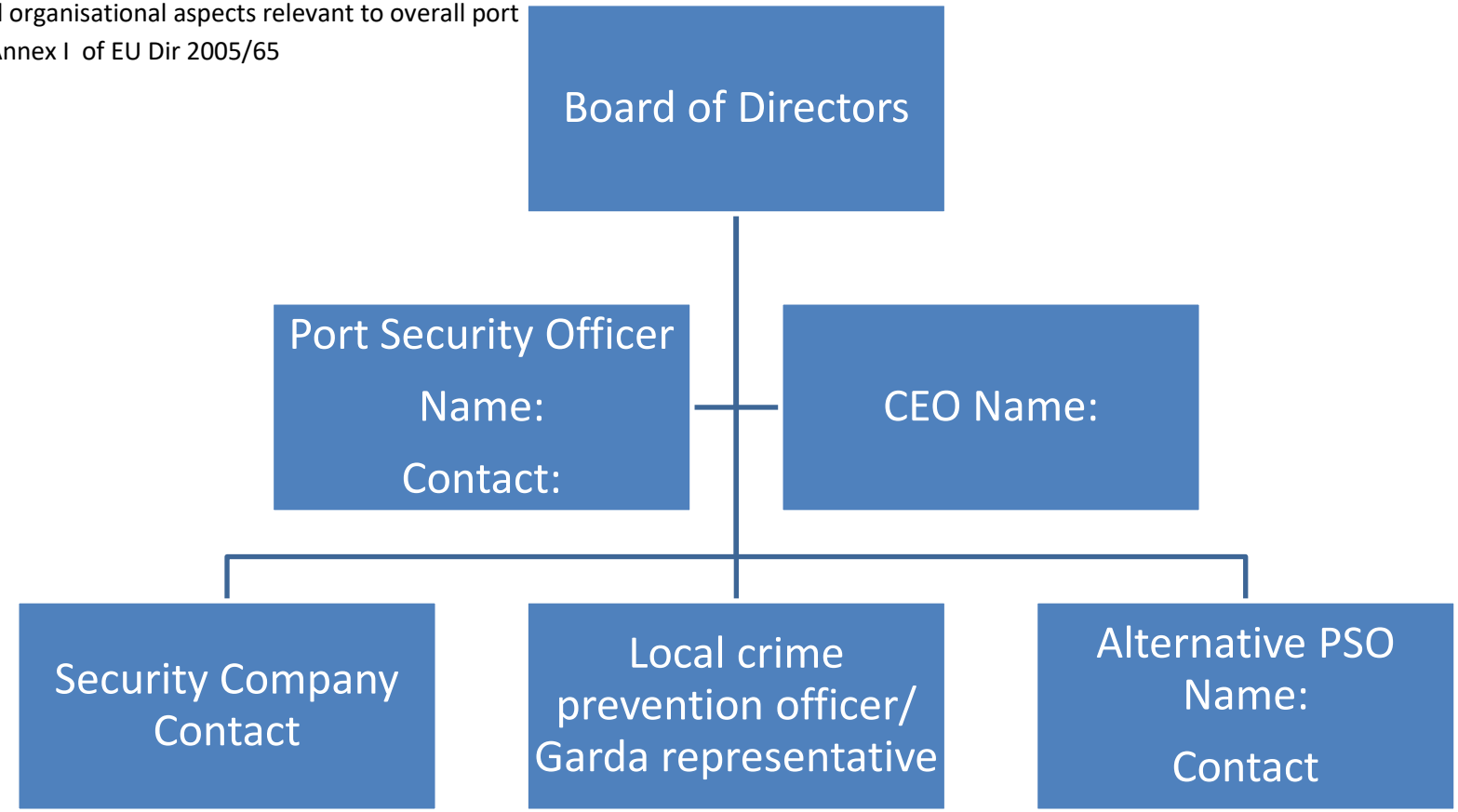
2.4 Port Boundary

Chapter 2 – 2.1 Port General Information

No.	EU Directive	General Information – Port	
5	-	Name of Port	
6	-	Port Point of Contact name(s) & phone number(s)	
7	-	PSO name & contact details. Has the PSO an approval letter issued by the MSO?	
8	-	Is there an alternative PSO? If Yes, give details	Yes ☐ No☐
9	-	Has PSO received security training, if yes, give details	Yes ☐ No☐
10	-	Name and contact details of local Garda Station / Crime prevention officer	

Chapter 2 –2.1 Organisational Structure

Identify all organisational aspects relevant to overall port security, Annex I of EU Dir 2005/65



No.	EU Directive	General Information – Port	
12		**Size and brief description of port including sub areas**	
13	**Annex I**	**No. of Berths and vessel types**	
14	-	**Hours of opening**	
15	**Annex I**	**Does the port handle Dangerous Goods? If yes, give details**	Yes ☐ No☐

Chapter2 – 2.2 Structural & Operational Information

No.	EU Directive	General Information – Port	
16	Annex I	Access Points to port Provide photos	
17	-	Have maps and aerial photos delineating the Virtual boundary as per Dir 2005/65 EC, the Ship/Shore interface boundary as per EU Regulation 725/2004 and Admiralty Charts showing adjacent water approaches to the port been provided?	Yes ☐ No☐
18	-	Have there been any structural or operational changes in the port since previous assessment?	Yes ☐ No☐ If yes, give details
19	-	Have there been any incidents recorded in the port's security log.	Yes ☐ No☐ If yes, give details

Chapter 2 – 2.3 Tenants and adjacent users

No.	EU Directive	General Information – Tenants and adjacent users	
20	Annex I	Name(s) of Tenants within the port boundary & Contact details (brief -full description to be submitted in Port Security Plan)	
21	Annex I	Name any adjacent facilities external to the Port Boundary and contact details (brief – full description to be submitted as appendix)	

Chapter 2 – 2.4 Port Boundary

Provide up to date aerial photographs, maps, drawings, plans & charts, as appropriate, outlining the delineation of the port boundary as per Dir. 2005/65 EC[4], including the port facility (ies) boundaries as per EU Regulation 725/2004. Include Admiralty Charts showing adjacent water approaches to the port.

Provide narrative detailing how the port boundary has been established taking into account the TAPs II Methodology and identifying all areas which are relevant to port security,

For Article 2.4 ports, before re-approval of the Art. 2.4 status is considered, the MSO will require clear evidence to be provided to clearly identify that the boundaries of the single port facility, within the meaning of Regulation 725/2004/EC, have been assessed and found to effectively cover the port in terms of security taking account of the TAPS II methodology.

The findings in relation to ongoing Art. 2.4 status are to be summarised in a concluding statement below.

- **…….**

[4] Refer to Annex 2 - Guidelines for the definition of port boundaries under Directive 2005/65/EC on enhancing port security and TAPS II methodology

Chapter 3 Port Security Assessment

3.1 Critical Assets

3.2 Important Assets and infrastructure

Chapter 3 – 3.1 Critical Assets

No.	EU Directive	Critical Assets – Port	
22	Annex I	Comment on structural integrity of the physical security measures e.g. fence condition, working lights, cameras etc.	
23	Annex I	List cargo facilities, terminals, storage areas and cargo handling equipment	
24	Annex I	List systems such as electrical distribution systems, radio and telecommunication systems, computer systems and networks	

Chapter 3 – 3.1 Critical Assets

No.	EU Directive	Critical Assets - identify all areas which are relevant to port security.	
25		List utilities, power plants, cargo transfer piping and water supplies	
26		List bridges, railways and roads infrastructure.	

Chapter 3 – 3.1 Critical Assets

No.	EU Directive	Critical Assets - identify all areas which are relevant to port security,	
27	Annex I	List security and surveillance equipment and systems	
28	Annex I	List any other operations taking place within or adjacent to port.	
29	Annex I	Identify risk variations based on seasonality/cargo etc.	

Chapter 3 – 3.2 Identification and evaluation of important assets and infrastructure which it is important to protect

No.	EU Directive	Identification and evaluation of important assets and infrastructure which it is important to protect				
30		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.	EU Directive	Identification and evaluation of important assets and infrastructure which it is important to protect				
30		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 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.

A port security assessment shall include, at least the following elements:

Dir. 2005/65/EC Annex I 1.1-1.4

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

- Damage to, or destruction of a port or of a 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 entrances, locks approaches etc.
- Nuclear, biological and chemical attack
- Possibility of cluster effects of security incident

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'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 and ships moving in the port *
   - 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 services and utilities
   - Measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks
   - 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 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

Chapter 5 Current Port Security Measures

5.1 Structural Port Security

5.2 Procedural Port Security

Chapter 5 – 5.1 Structural Port Security Measures

No.	EU Directive	Structural Security Measures	
31	Annex I	List any areas which if damaged or used for illicit observation, may pose a risk to persons, property or operations within the port	
32	Annex I	Brief details of any passenger or vehicle security arrangements (e.g. boarding cards, restricted areas, screening, searching)	
33	Annex I	Outline security clearance standards, specifically "need to know" requirements of those directly involved	
34	Annex I	Brief details of cargo handling security arrangements	

Chapter 5 – 5.1 Structural Port Security Measures

No.	EU Directive	Structural Security Measures	
35	Annex I	Identify all security infrastructure including: Fences, Access gates, Entry control points, High level lighting, CCTV cameras (fixed, tilt, IR etc.)	
36		Identify CCTV storage locations	
37	-	Period of time footage is stored	
38	-	Comment on the protection of communications hub	

Chapter 5 – 5.2 Procedural Port Security Measures

No.	EU Directive	Procedural Security Measures	
39	-	**Is there a previously approved Port Security Assessment as per Directive 2005/65 EC**	Yes ☐ No☐
40	-	**Is there an approved Port Security Plan.** **If Yes, where is it stored and what personnel have access?**	Yes ☐ No☐
41	Annex I	**Brief details of any existing arrangements with private security companies.**	
42	Annex I	**Is the security company approved in accordance with requirements of the Private Security Services Act, 2004?**	Yes ☐ No☐

Chapter 5 – 5.2 Procedural Port Security Measures

No.	EU Directive	Procedural Security Measures	
43	Annex I	List personnel security systems (e.g. clearance, ID, alarms, types of passes)	
44	Annex I	Identify which port 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	
45	Annex I	How often is personnel security pass system audited?	
46	Annex I	Is there an out of hours security patrol? If yes, give details	Yes ☐ No☐

Chapter 5 – 5.2 Procedural Port Security Measures

No.	EU Directive	Procedural Security Measures	
47	Annex I	Provide list of restricted areas within the Port	
48	-	Provide list of assembly points	
49	Annex I	List available security staff & additional equipment provision in the event of Level 2 or Level 3 security incidents	
50	Annex I	Detailed maritime security training to port staff and contractors	
51	Annex I	Is there a system of maritime security drills, exercise & auditing in place? Details	Yes ☐ No☐

Chapter 5 – 5.2 Procedural Port Security Measures

No.	EU Directive	Procedural Security Measures	
52	Annex I	Procedures for adapting and updating the port security assessment and plan	
53	Annex I	Procedures for protecting sensitive and restricted information either electronically or in paper form	
54	Annex I	Identify how measures, procedures and actions will be reinforced in the event of an increase in security level	
55	Annex I	Specific requirements for dealing with established security concerns such as suspect cargo, luggage, bunker, provisions or persons unknown parcels, known dangers (bombs), UAV's / drones	

Chapter 5 – 5.2 Procedural Port Security Measures

No.	EU Directive	Procedural Security Measures	
56		**Has the Port Administration 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)**	
57		**Are measures in place for protecting electronic operational systems, security pass systems, records etc**	
58		**Are port staff trained in cyber security awareness?**	

No.	**EU Directive**	**Identify measures at Security Level 1 encompassing Directive 2005/65** (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.**
59			

No.	**EU Directive**	**Identify additional measures at Security Level 2 encompassing Directive 2005/65** (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.***	
60			

No.	**EU Directive**	**Identify further additional measures at Security Level 3 Directive 2005/65** (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.**
61			

Chapter 6 Port 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, including each facilities ship/shore access, details of all relevant assets including vessel traffic monitoring hubs.

A risk analysis should be included in the waterside 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.	EU Directive	Waterside Assessment General Information	
62	Annex I	Provide a brief description of the overall area involved	
63	Annex I	List anchorages, channels, manoeuvring & berthing areas	
64	Annex I	Brief description of port and individual port facilities adjacent water approaches. Provide photos as appropriate.	

No.	EU Directive	Waterside Assessment General Information	
65	Annex I	List Port vessel traffic management systems & aids to navigation	
66	Annex I	List port service vessels including pilot boats, tugs & lighters etc.	

Chapter 6 – 6.3 Waterside assets & infrastructure

No.	EU Directive	Important assets and infrastructure				
67		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.	EU Directive	Important assets and infrastructure				
67		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 Identification of Vulnerabilities & Recommendations

Identification of vulnerabilities & Recommendations		
No	**Area/Topic**	**Recommendation**

Identification of vulnerabilities & Recommendations		
No	**Area/Topic**	**Recommendation**

Checklist

Name of Port:			**Date:**		**Issue Number:**
Port Security Plan	☐	Security personnel	☐	Physical security	☐
Communications systems	☐	Lighting	☐	Navigation systems	☐
Port operations	☐	Infrastructure and services	☐	Stores	☐
Intruder alarm systems	☐	Designated port area	☐	Security levels 2 & 3	☐
CCTV systems	☐	Restricted areas	☐	PSO Approval from MSO	☐
Access control systems	☐	Water approaches and patrols	☐	Cluster Effects considered	☐
Security patrols and manning	☐	Access to ships	☐	Cyber Security Measures	☐
Security awareness training	☐	Port personnel procedures	☐	UAV's / Drones considered	☐
Security organisation and Management	☐	Ship personnel	☐		☐
Berths (not covered by PFSP)	☐	Cargo	☐		☐
Document Check list					
Drawings of port boundary & narrative referencing use of TAPS II methodology	☐	Lighting footprint	☐	CCTV locations	☐
Aerial photos delineating port boundary	☐	Photos of access points	☐	Critical infrastructure	☐
		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. **Guidelines for the definition of port boundaries under Directive 2005/65/EC on enhancing port security**
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. Guidelines for the definition of port boundaries under Directive 2005/65/EC on enhancing port security

Introduction

The first report assessing the implementation of Directive 2005/65/EC - adopted in 2009 by the Commission[5] - considered that a significant number of Member States faced difficulties to achieve the full practical implementation of the Directive, due by 15 June 2007. One of the main difficulties remained the definition of the boundaries of the port in terms of security. This difficulty was reflected in the variety of approaches adopted by Member States in determining the boundaries of the ports falling under the scope of the Directive.

Following the conclusions of this report, the Commission entrusted its Joint Research Centre[6] (JRC) to conduct a study with main focus on methodologies and technical means for efficient implementation of the Directive (Study on Technical Aspects of port Area Security – TAPS II). The definition of port boundaries is one of the core issues addressed in this study which identified the various relevant parameters (Section 2) and developed a methodology (Section 3) based on a systemic process for port boundaries definition.

The definition of port boundaries is naturally linked to port security assessments and plans. In accordance with Article 10 of the Directive, Member States shall ensure that the port security assessments and the port security plans are reviewed at least once every five years. In the conclusion of its second report[7] assessing the implementation of Directive 2005/65/EC, the Commission considers that the use of the methodology developed in the TAPS II study could be useful, where necessary, in order to redefine the perimeter of ports.

These guidelines for the definition of port boundaries have been agreed by the Member States delegates within the MARSEC Committee.

Parameters affecting port boundary definition (TAPS II study)

Port cohesion elements

As a real synergic system, the port cannot perform its functions without the contribution of a set of activities and/or services. The security of the port system depends on the vulnerability of each of its components, regardless their location.

In terms of planning and implementing security measures, a port, as any other system or organisation, has much more control on its internal components than on the external systems/ services.

[5] COM(2009)2 final
[6] DG JRC - Institute for the Protection and Security of the Citizen (IPSC) – Maritime Affairs Unit
[7] COM(2013)792 final

Directive 2005/65/EC complements the security measures introduced by Regulation (EC) No 725/2004 on enhancing ship and port facility security by expanding a security regime to the entire port and goes beyond the ship/port facility interface. There are some basic elements that glue together various areas, activities, installations, infrastructures or organisations in one entity which is commonly understood as a port.

Before detailing any considerations on how and where to fix the port security boundaries, it is important to have a common approach as to when port or other facilities, terminals, installations, marinas etc. are part of a single port in terms of security requirements and when they are not. The factors that contribute to such a decision are common essential port element considered as ***cohesion elements***. A non-exhaustive prioritised generic list of such cohesion elements would be:

1. Common main port infrastructure like breakwaters, seawall etc.;
2. Common essential port services such as pilotage, towage, mooring, boatmen (commonly known as technical-nautical services);
3. Common water zones, seaward and inland waterways and anchorages;
4. Common inland access (road and railways) and networks;
5. Common general port services like bunkering, water supply, waste reception, ship chandlers, repair & maintenance services, ICT support;
6. Common emergency services and waterside traffic control systems (VTS), usually performed by a single entity for the entire port area;
7. Common supporting services as shipping agents, freight forwarders, banks, insurance companies, private security companies, railway and bus operators etc.
8. Other geographic, orographic, morphological aspects and port layout.

Port or other facilities, installations, entities or areas sharing such elements participate, as a matter of fact, the same systemic entity (the port) and should be considered in the same port security assessment and plan.

Such port cohesion elements can be identified and evaluated, for each specific case, at the very beginning of the Port Security Assessment - PSA[8].

Type of port facility, area or infrastructure

The classification of ports can depend on several factors: freight type (passenger, ferry, bulk, oil, gas, container, poly-functional), geographical location, sea and land access, urban aspect or administration model.

The definition of the port boundaries depends on the typology of the port as well as on the type of the terminals, infrastructure, and installations. Highly critical ports, terminals or port areas should imply:

- A more complex approach in terms of developing the risk assessment, taking in due consideration all port characteristics, vulnerabilities and potential impacts inside and outside the port;
- More effective security measures according to the three security levels;

[8] Directive 2005/65/EC on enhancing port security, Art. 6.

- Eventual inclusion of additional adjacent areas under the port security regime in order to enhance the port global security according to the PSA.

Port size

Regardless of their size, ports usually have the same structure and service typology. Small ports are not as complex as big ports; and even though the relations between the services, Public Authorities, stakeholders and hosting cities can be simpler, the port boundaries definition process does not differ significantly. Minor complexity can lead to easier solutions and can reduce the time necessary for the process of defining boundaries.

Major ports have often a very complex layout where a variety of activities, industries, communications and urban areas coexist as a result of progressive development during decades or centuries. These are mostly multipurpose ports and can hardly be classified differently. This increases the complexity of the *harbour* layout and functions and of the interrelations between Authorities or other Entities.

Administrative port boundaries

The port, as an entity, is defined as the totality of elements and activities composing it, giving a complete description of its boundaries. A good starting point is to first consider the port's administrative limits and then evaluate if they are consistent with port security purposes for future planning. In most cases, the administrative limits define the ownership of the State or other Public entities, but have not been intended for security purposes. The definition of the port perimeter according to its main activities, services and purposes indicates an approach which is compatible with the port as a functional system.

Cross vulnerability

The vulnerability of port areas depends on their own security parameters as well as on the vulnerabilities of port areas and facilities they are adjacent or interacting with. Moreover, the vulnerability of the whole port is affected by the vulnerability of every single facility or port area. The presence of dangerous goods has to be carefully considered throughout the port and not only evaluated in a Port Facility Security Assessment - PFSA[9].

Port area permeability

Potential attackers could find an easy gap in the port security system in an adjacent area to their final real target. Port areas having a high rate of permeability to external agents, even if they have not a high rate of intrinsic criticality, are a challenge for the entire port security system.

Homogenous & continuous security measures

Security should be homogenous and continuous to be effective. When some areas are protected and others are totally open and unprotected, the latter are the weakest link and can affect the security of

[9] Regulation (EC) No 725/2004 on enhancing ship and port facility security – Annex II (International Code for the security of ships and of port facility – ISPS code), Section A/15.

the entire port. Zones/ areas inside the port security boundaries may be included for the sake of continuity.

Port area clusters

According to Annex II of the Directive, not all port areas require the same preventive measures and have the same access requirements. Clusters of port areas can be defined in order to apply homogenous security measures.

Security levels [10]

The port security plan (PSP[11]) provides security measures to be enforced according to 3 security levels. For some areas access control or security requirements should enter into force only at security level 2 or 3. Many areas can be totally open according to their access requirements or port layout as being urban areas or public infrastructures and they do not need to be closed at security level 1. However, these areas should be included in the port security boundaries in order to be able to apply access restrictions when needed.

Additional remarks

Before tackling the main issue of this section, below are some remarks and observations.

Water port access / area

Article 3 (1) of Directive 2005/65/EC states that “port” means 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. The words "land" and "water" have to be carefully taken into consideration. If the Port Facility Security Plan - PFSP[12] primarily considers the land boundaries, then the PSP should equally consider the water area to be of an added value for the security of port facilities.

Water area provides common sea (river/canal) access to port facilities and other port areas contributing significantly in the integration of the entire port system. Water area is a very strong cohesive element which should be taken into high consideration when defining port boundaries.

Port security sectors

Port areas can be often divided in quite homogenous sectors. In some ports, the existence of a group of adjacent port facilities (PFs) allows the creation of a conveniently fenced and

[10] Directive 2005/65/EC on enhancing port security, Art. 8.
[11] Directive 2005/65/EC on enhancing port security, Art. 7.
[12] Regulation (EC) No 725/2004 on enhancing ship and port facility security – Annex II (International Code for the security of ships and of port facility – ISPS code), Section A/16.

closed secure sector that includes more than one PF and can be entered through one or more gates.

It is possible to define homogenous areas where access control can be applied or, if not, where other homogenous security measures can be implemented. That is to say that it is possible to define clusters of similar areas as far as access requirements, risk assessment and other involved parameters are concerned.

TAPS II methodology

The proposed methodology is the result of a **systemic approach** where the port is considered as one complex entity whose security or vulnerability depends on all its components. It should be applied to all relevant ports under Directive 2005/65/EC[13].

The methodology consists of 2 fundamental checks/ controls described in the 2 loops in Figure 1. The first defines which port facilities and other elements are to be considered as a part of the same port, while the second defines the effective port security boundaries through security analysis.

The first step of the process is to check if the port, as defined initially, e.g. considering the port administrative boundaries, is effectively a stand-alone port or if it must include additional port facilities. The criterion is sharing one or more essential port elements (or port cohesion elements, as outlined in section 0) with one or more other port facilities. If two or more port facilities share water access, inland access and other essential services, they are likely to be part of the same port. On the contrary, if a port facility is isolated, with none of its essential elements being common to any other port facility, then this first loop can be avoided.

After deciding which port facilities are to be included in the port, the process continues with the second loop to define the port security boundaries. To fulfill the role of port security boundaries, the port reference boundaries (in most cases, administrative) are considered and then - if necessary – they are modified as required. An iterative process is used to consider the port layout and area clustering, along with the vulnerabilities, cross vulnerabilities and impacts analysis. Following the process, additional areas can be included or not within the port security boundaries. It must be noted that the inclusion of certain areas within the port security boundaries does not imply their protection or the application of access restrictions. This can be part of the port security plan and can vary according to the security level considered.

[13] Ports in which one or more port facilities are covered by an approved port facility security plan pursuant to Regulation (EC) No 725/2004 – see Directive 2005/65/EC - Article 2(2).

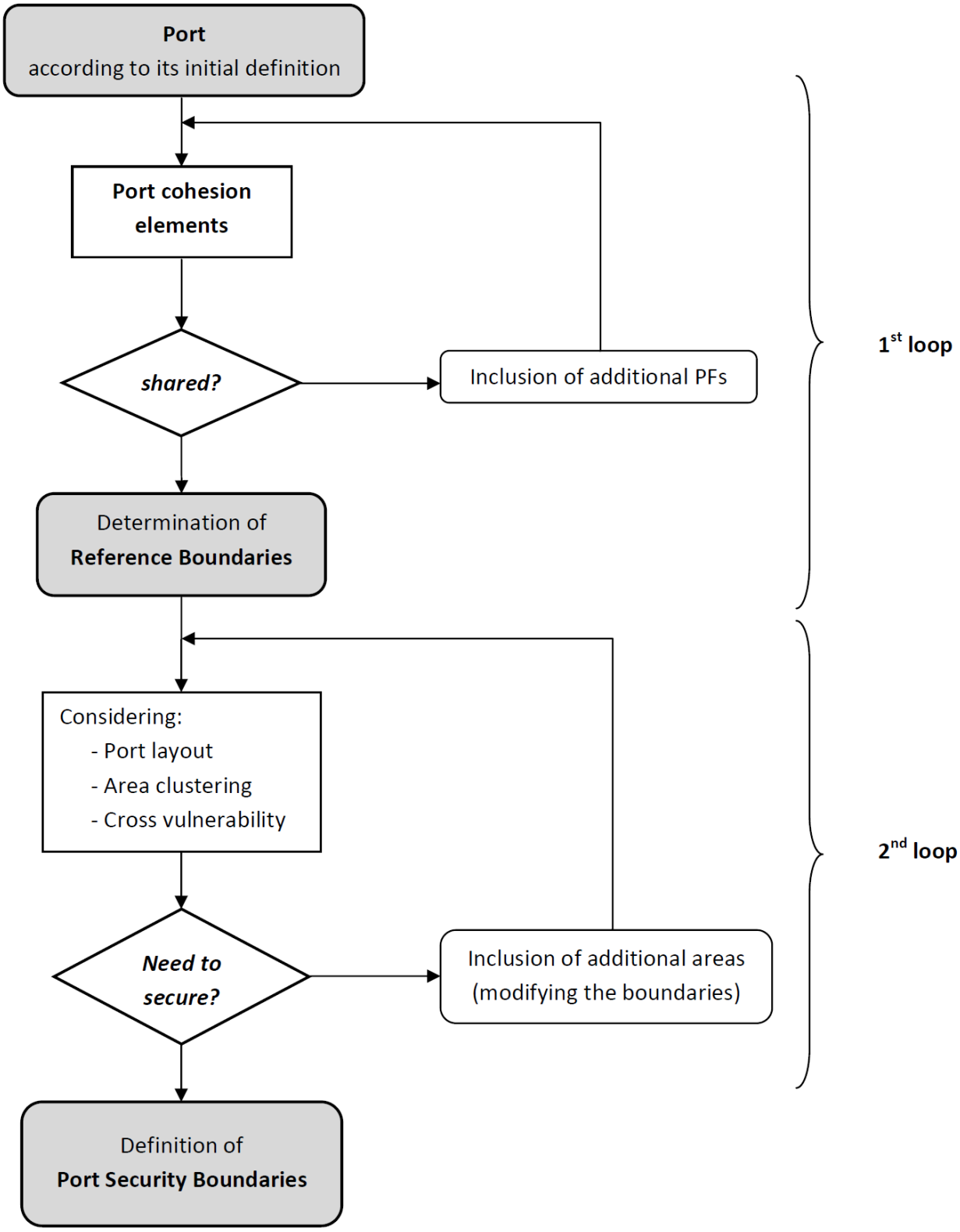


Figure 1: Port security boundary definition process flow-chart

Each of the above steps is further explained in the following subsections:

Port constitutive elements & reference boundaries

The first step consists of the identification of all the essential elements of the port by listing all port facilities including marinas, fishing ports and any other facility, coast/location with port functionality within a region where interactions could be expected.

Table 1 in its first column shows all essential port elements considered as port cohesion elements, mapped against each of the port facilities listed. Typically, such elements include water zones, sea access, land access, essential infrastructure and services. The scope is to identify the relation and the interdependencies in order to verify if those port facilities are part or the same port.

Table 1 provides an example, Port A, for which the security boundaries are to be established could potentially have common elements with port facilities PF 1, PF 2, PF 3 and PF 4. All these entities are placed in the column headers, while the port cohesion elements are in the line headers. All essential / cohesion elements of Port A are identified in the 2nd column. For each of the port facilities listed in the remaining column headers it is considered if they share the Port A's essential / cohesion elements. Accordingly, each of the cells of the table is filled with one of the following marks:

FS → Share fully, if the element of cohesion is, at a great extent, shared with Port A
PS → Share partially, if the element of cohesion is only marginally shared with Port A
-- → No sharing, if the element of cohesion is not shared at all with Port A

The color of the PF xx column should be an indication as to if PF xx should be considered or not within the Port A. For example, according to Table 1, PF 1 should clearly be part of Port A, PF 2 should also be included, whereas PF 3 and PF 4 are not.

<u>If Port A includes PF 1 and PF 2 the boundaries[14] of PF 1 + PF 2 + relevant areas of essential/cohesion port elements constitute the port reference boundaries--starting point for the subsequent analysis</u>.

Table 1: Example of mapping of the essential port constitutive elements between the target port and neighbouring port facilities[15]

Cohesion Elements	Port A : Identification	PF 1	PF 2	PF 3	PF 4
Main infrastructure	Breakwater, dockside	FS	PS	PS	--
Essential services	Pilotage, towage, mooring, boatmen	PS	PS	PS	PS
Water zones	Corridor as per map, anchorages	FS	PS	--	--
Inland access	Access to national highway	PS	PS	--	--

[14] Usually the administrative or the property and boundaries and the boundaries of the associated water zones.
[15] For the purposes of this table, port facilities include also marinas, fishing ports and other facilities with port functionality.

General services	Bunkering, supplies, waste reception	PS	PS	--	--
Emergency services	…..	FS	FS	FS	FS
Supporting services	….	PS	PS	PS	PS
Other	……	PS	PS	PS	PS

Identification of port assets and infrastructures

In order to define the final port security boundaries, after considering the reference boundaries, common port essential elements and port facilities including marinas, fishing pears and shipyards, other elements (areas, assets and infrastructure) should be identified for security reasons. These elements are not necessarily port areas.

Areas to be protected can be also outside the reference port boundaries (e.g. power supply or water, physical and cyber-based essential systems, emergency services, etc.). Areas hosting such important elements have to be included in the PSP even if they are disconnected, i.e. physically outside the port.

All these areas/ elements have to be identified and marked on the port plan or map in order to proceed with the third step which concerns the port layout.

Verifying the port layout

After defining essential port assets and infrastructure, the evaluation of the port layout is an important stage to verify the resulting port security boundaries. Port security limits should, ideally, contain all port facilities, all essential port elements, assets and infrastructure. However, in order to fulfill their security role, they must also be practical and manageable[16].

As a logical consequence of the port layout evaluation and depending on the location of facilities and relevant areas, it is possible to verify potential crossed vulnerability relations between port portions. In this case, an appropriate evaluation should verify the opportunity to include additional areas which could affect the security of the port. A relevant example is that of connected water zones: sometimes it is impossible to reach a very well confined port facility from the landside, while it could be simple to do so from the water. The inclusion of port water areas has to be carefully considered not only according to the specific facilities they are related to, but also following another logical procedure: waters inside the same seaside protective structures have a strong cohesion. The same concept applies to anchorages or waterways. It is also important to stress that marine **traffic monitoring systems,** useful and used not only for safety reasons but also **for security purposes**, are managed by the Authorities for the entire port area. This can be considered as an additional cohesion element.

Another circumstance is the existence of urban or other totally open areas, very close to port facilities or to other sensitive inland or water areas. Port areas, especially **obsolete or**

[16] For example, fragmented boundaries are difficult to manage and should, in general, be avoided.

abandoned facilities, converted to recreational centers, museums, cinemas, recreational activities, shops or supermarkets, which are not intended to perform a "port function" anymore, could be excluded from port security boundaries.

If an area is completely or partially excluded from the port security boundaries, this cannot affect its safety or security. Member States have to guarantee that **equivalent controls and security measures** are applied in such areas to ensure that they are at least as effective as those prescribed for similar areas outside the port.

In the end of the process, due to identified crossed vulnerabilities or the port layout, extra areas have to be included inside port borders even if they are not directly related to the port activities. This can also be due to the need to take into account the orography, road network or port infrastructure.

Those additional areas are listed in Table 2. The first and second columns identify and organize the elements, while the third prioritize their inclusion within the port security boundaries. Accordingly, each of the cells of the 3rd column is filled with one of the following marks:

1 → Priority 1: to be included
2 → Priority 2: to be considered
3 → Not to be included

Areas not considered in this process will be out of the application of any security measures and will not contribute to the security of the port at all.

Table 2: Additional areas / assets / infrastructure, potentially included within the port security boundaries

Area classification	Additional elements	Priority
A 1 (non-operational)	Power supply, sector 1	**1**
A 2 (non-operational)	Industrial area, sector 2	**2**
A 3 (public)	Restaurants, shops and pubs, sector 3	**3**
A 4 (public)	Parking, sector 4	**1**
A 4 (public)	Railways station, sector 3	**2**
A 5 …..	….. ……	**….**

Port typology, size and area clustering

The port typology, PF type, categories of traffic and activities performed within the port borders, are other parameters to be considered when assigning the priorities. Railways and rail accesses will necessarily have an impact on a container port, while pipelines and other similar devices will characterise an oil port.

A careful consideration should be given to the presence (permanent or occasional) of dangerous goods or hazardous materials, not only for maintaining an acceptable security

level, but also for evaluating and containing the potential negative effects of a security incident. In case of high-risk facilities, the necessity to have a more effective "double barrier" can result in the inclusion of additional inland or water zones in the port area according to PSA.

The systemic approach calls for the inclusion within the security port boundaries of all the areas that have a significant role in the economy of the port or where important assets are located. Different areas may have different access requirements. Many of them can be totally open to the public, at least at security level 1.

Permeability to external agents has to be considered under a more complex point of view and be compared with access needs and access restrictions[17]. Interaction of non-homogenous activities inside an area or a system could amplify risks. Inside the port area, as far as access control is concerned, clusters of homogenous areas need to be identified.

Clustering similar areas (with analogous security requirements) has obvious scale effects. Table 3 shows an example of possible homogenous areas and applied security measures.

Table 3: Port security area clustering

Port Security Clusters	Areas	Access requirements	Access control Level #1	Access control Level #2	Access control Level #3	Other security measures
CL #1	PF1, PF2 PF3	Access reserved to authorised personnel (permanent, trusted, occasional)	Access control: Procedures; Technical means On car, trucks & pedestrians; Etc.	Access control: Procedures; Technical means On car, trucks & pedestrians; Etc.	Procedures; Technical means On car, trucks & pedestrians; Etc.	Video surveillance SL 1-3); Patrolling (SL 2-3)
CL #2	Public area sector 1	Open for public use (unlimited, non-identified)	No access control;	No access control;	Access control: Procedures; Technical means On car, trucks & pedestrians; etc.	Signage; Public awareness; Other security measures patrolling (SL 3)
CL #3	….. …..	….. …..	….. …..	….. …..	….. …..	….. …..

In addition, the relevant port security objects can be classified in clusters according to the expected effects of a potential incident, thus the following categories can be identified:

Cat. A: objects whose intentional disturbance would cause many victims, disturbance of national economy, considerable damage to the environment and a shock to the society;

Cat. B: objects whose intentional disturbance would cause some victims, disturbance of regional economy, substantial damage to the environment;

[17] TAPS II study, section 4.8 – table 4.

Cat. C: objects whose intentional disturbance would cause no such damage as specified for cat. A-B.

Such clusters can be useful while deciding which security measures have to be applied to port areas. They will be the result of a complex assessment which has to include, among other factors, a crossed evaluation of access requirements and of the most probable consequences of potential incidents.

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[18] 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

[18] 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)

it comes to access control and cargo handling. Some ports may already be concerned by the cybersecurity requirements put in place by the NIS Directive[19] and the subsequent NIS 2 Directive[20].

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[21], 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

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*"

[19] 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)
[20] 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)
[21] 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

- 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[22], 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

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[23]. 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[24] 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

[22] Regulation 725/2004, Annex II, Paragraph 16.1
[23] Regulation 725/2004, Annex III, Paragraph 15.6
[24] ibid

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 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"[25].

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[26]. An "incident" under the NIS 2 Directive has a wider meaning and may concern incidents that are not deliberate cyber attacks[27]. 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[28] 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[29].

Port facility security plan

[25] Directive 2022/2555, Article 6 (15)
[26] Regulation 724/2004, Article 2 (13)
[27] See Directive 2022/2555, Article 6 (6)
[28] "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
[29] See internet links: Guidelines - Cyber Risk Management for Ports — ENISA (europa.eu) and Cyber risk management for ports — ENISA (europa.eu)

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[30].

Based then on the results of the PFSA, there may be several aspects that the PFSP should address when considering cybersecurity[31], and which are described below.

Security organisation of the port facility[32]

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).

Links with other authorities[33]

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

[30] Regulation 725/2004, Annex II, Paragraph 16.1
[31] 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"
[32] Regulation 725/2004, Annex III, Paragraph 16.3.1
[33] Regulation 725/2004, Annex III, Paragraph 16.3.2

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[34].

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

The PFSP should detail if additional cybersecurity measures are to be put in place at security level 2 and/or 3[35]. 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[36].

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[37]. 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[38].

According to Regulation 725/2004, a "security incident" means any suspicious act or circumstance threatening security, of a port facility in this case[39]. In the NIS 2 Directive, an

[34] ibid
[35] Regulation 725/2004, Annex III, Paragraph 16.3.4
[36] Regulation 725/2004, Annex II, Paragraph 16.3.9
[37] Directive 2022/2555, Article 23 (1)
[38] Directive 2022/2555, Article 30
[39] Regulation 725/2004, Annex I, Regulation 1, Paragraph 1.13

"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"[40].

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[41]) 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 or changing circumstances[42]. 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[43].

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.

[40] Directive 2022/2555, Article 6 (6)
[41] See definition in Directive 2022/2555, Article 6 (5)
[42] Regulation 725/2004, Annex III, Paragraph 16.3.5
[43] Regulation 725/2004, Annex II, Paragraph 15.4

Drills and exercises

As drills should test individual elements of the PFSP[44], 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.

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[45] 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[46] 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[47], 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.

[44] Regulation 725/2004, Annex III, Paragraph 18.5
[45] See internet link: Cybersecurity (europa.eu)
[46] Regulation 725/2004, Annex III, Paragraph 18.1.9
[47] Regulation 725/2004, Annex III, Paragraph 18.2.1

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[48].

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[49].

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[50].

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

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.

[48] Regulation 725/2004, Annex III, Paragraph 16.8.2
[49] Regulation 725/2004, Annex III, Paragraph 16.8.6
[50] Regulation 725/2004, Annex II, Paragraph 16.7

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[51].

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.

[51] Directive 2005/65, Annex II

Conclusion

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.