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

Introduction

The European Commission has found it useful to develop 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 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

[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)

[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

document will assist Member States and port facilities/ports to take on challenges relating to cybersecurity.

The European Commission presented a final draft of this guidance to Member States in the 89th meeting of the Committee for Maritime Security, after previous consultation. This guidance is now presented to member organisations of the Stakeholders Advisory Group on Maritime Security.

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*"

- 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

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

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

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 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].

---

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

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.

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

Security levels

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].

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

[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
[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)

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[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.

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

[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
[28] See internet link: Cybersecurity (europa.eu)

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].

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

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

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

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.

[34] 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.