EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR MOBILITY AND TRANSPORT
Directorate A - Policy coordination
A.5 - Security

European Maritime Safety Agency

MARSEC Doc. 9209

Guidance on how to address cybersecurity onboard ships during audits, controls, verifications and inspections

DISCLAIMER

This document has been developed by the European Commission with the assistance of the European Maritime Safety Agency with a view to providing to EU Member States' Maritime Administrations/Designated Authorities guidance in addressing cybersecurity onboard ships during security-related audit and inspection activities.

The document does not have a regulatory purpose. None of its content is binding in nature or should be interpreted as superseding any legal/regulatory framework governing the implementation of maritime security in the Member States, be it national, European or international, more particularly the maritime security requirements of Regulation (EC) No. 725/2004.

This document is not a manual covering all aspects of cybersecurity in the Regulation.

This is a living document that will be revisited within the MARSEC Committee when considered necessary at the initiative of the Commission.

The guidance in this document should always be considered subject to and in conjunction with reference to the Member States' specific regulatory and operational contexts and any other relevant circumstances.

The content of this document is not restricted but it is intended for the use of all personnel responsible for security in the EU maritime sector. Therefore, the dissemination of the content is not limited but encouraged. In this regard, national administrations are advised to share this document with those in the private sector that might benefit from it (i.e., Port Facility Security Officers, Company Security Officers, etc).

Table of Contents

1. Introduction

The European Commission has found necessary to develop this guidance document to clarify the legislative requirements concerning cybersecurity onboard EU Member State flagged ships, taking into consideration the requirement set at EU level by Regulation (EC) No 725/2004 of 31 March 2004 on enhancing ship and port facility security and the incitation at IMO level to address it within the context of the ISM Code (i.e. Resolution MSC 428 (98)).

The present document offers guidance for the cybersecurity related elements that should be assessed during maritime security inspections on EU Member State flagged ships, within the framework of Regulation (EC) No 725/2004. The initial draft was prepared by the European Maritime Safety Agency, which provides technical assistance to the European Commission on maritime security, as foreseen by Art. 2.2.b of the EMSA founding Regulation. While the various documents included in the "Relevant Documents" section at the end of this paper provide guidance to the industry, there are limited elements for maritime security inspections on how and what to assess in regard to cybersecurity, which falls under Annex III, Paragraph 8.3.5 of Regulation (EC) No 725/2004 of 31 March 2004, made mandatory under Art. 3.4 of this Regulation.

It should be noted that this document **does not set any legal requirements**. The European Commission notes that guidance material already exists on cybersecurity in the maritime sector[1]. However, 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 the EU maritime security legislation is focused on physical security, but nevertheless provides a useful framework through which to consider where cyber-protective measures may be the most useful, especially these days, where ships are becoming increasingly digitalised.

The European Commission hopes that this document will assist Member States and their maritime security inspectors (Flag State/RSO surveyors/auditors) to take on challenges related to inclusion of cybersecurity elements in inspections on EU Member State flagged ships.

This document was finalised during the 92nd meeting of the EU Maritime Security Committee, on 8 November 2023, and is considered a living document to be revisited in the EU Maritime Security Committee when considered necessary.

[1] A list of relevant publications is included in the Reference section.

2. Legislative requirements

2.1. Regulation (EC) No. 725/2004: Annex III, Paragraph 8.3.5

"A SSA should address the following elements onboard or within a ship: […] radio and telecommunication systems, including computer systems and networks[2]".

- This means that a Ship Security Assessment (SSA) must consider the security of the ship's computer systems and networks, which is understood to mean "cybersecurity", as all systems on board a ship are potentially vulnerable to cyberthreats.

- Consequently, the resulting Ship Security Plan (SSP) must include the development of measures to address the cybersecurity vulnerabilities identified in the SSA. If cybersecurity is addressed in any other existing documentation, such as the ship's Safety Management System (SMS), as encouraged by the IMO MSC.428 (98), a cross-reference in the SSP would suffice.

- Member State inspections and verifications may then verify these measures, as the minimum needed to be in conformity with the legislation.

Based on this mandatory, for EU Member State flagged ships, paragraph, this document provides detailed guidance on how to address cybersecurity onboard ships throughout the mandatory paragraphs of Regulation (EC) 725/2004.

3. Guidance for security-related ship audits, controls, verifications, and inspections

Security is addressed under the ISPS Code for global shipping and Regulation (EC) 725/2004 for the EU Member State flagged ships, specifically. Cybersecurity is included in the aforementioned documents, as illustrated in the previous section. However, cybersecurity, and cyber risk specifically, should be addressed within the context of the ISM Code, according to the IMO Res. MSC. 428 (98). This discrepancy creates ambiguity during security-related ship audits, controls, verifications, and inspections carried out within the Regulation (EC) 725/2004 context.

The guidance presented in this section, albeit based within the context of Regulation (EC) 725/2004, adopts a broader approach, and as such, is applicable to any activity (audit, control, verification, inspection, under ISM and ISPS Codes) that addresses cybersecurity.

[2] By "computer systems and networks" all software-enabled systems onboard ships, falling under both IT and OT, are perceived to be included. A non-exhaustive list includes communication and navigation systems, integrated bridge systems including propulsion control, cargo and crew management systems, machinery management, power control systems, access control systems, etc

3.1. Regulation (EC) No. 725/2004

As according to IMO Res. 428(98) cybersecurity and cyber risk should be addressed within the context of the ISM Code and to avoid unnecessary duplication of effort, a possible way of addressing the regulatory requirement of Regulation (EC) 725/2004, as stated above, is to include a cross-reference to the relevant ship SMS content[3], in the SSP[4].

3.1.1. Ship Security Assessment

Those involved in preparing the SSA should be able to liaise with the designated personnel for the cybersecurity of the ship, onboard and/or in the shipping company's offices. If there is a lack of expertise, they should draw on the expertise of cybersecurity experts. This is in line with Annex III Paragraph 8.4.11 of Regulation (EC) 725/2004. It is worth pointing out that the requirement to be able to draw on expert assistance in relation to radio and telecommunication systems, including computer systems and networks is mandatory for EU Member States, according to Reg. 725/2004, Art. 3.4.

In considering cybersecurity in the SSA, the unique Information Technology (IT) and Operational Technology (OT) environment of each ship should be taken into consideration. In principle, higher reliance on IT and OT systems should entail a higher cybersecurity risk since the consequences of a potential cyber incident would be far more disruptive.

One possible way of satisfying the requirement of Annex III Paragraph 8.3.5 of Regulation (EC) 725/2004 is to include cybersecurity threat scenarios in the SSA, in the risk analysis of vulnerabilities[5]. The extent and detail of these scenarios will depend on the complexity of the unique environment of each ship.

It is also important to identify equipment and technical systems the sudden operational failure of which may result in hazardous situations and are therefore key to the operational functioning of the ship. Such equipment and technical systems, for example GMDSS/GNSS, bridge systems, loading and stability computers, engine control room console, fleet management software etc. should be cyber risk assessed, to identify how they could be vulnerable to cyber incidents.

Maritime cyberthreats should be considered and treated as any other maritime security threats. Consequently, in order to satisfy the requirement of Annex III Paragraph 8.3.5 of Regulation (EC) 725/2004 for cybersecurity, the SSA should follow the same process as for other maritime security threats and, therefore, address at least the minimum aspects, as stated in Annex II

[3] The content of the SMS related to cybersecurity, or other documentation where cybersecurity measures are set out, should be available to maritime security inspectors/auditors/surveyors during their visits onboard.

[4] The need for a cross-reference is stated in para. 4.10 of the Report of the Maritime Safety Committee on its 101st Session (MSC. 101/24) 12 July 2019. The cross-reference in the SSP should be in terms of page/chapter/paragraph or could also include a summary of the content included in the SMS, depending on specific instructions issued by each Member State.

[5] Alternative ways of assessing risk include threat mapping, quantitative/qualitative risk assessments etc.

Article 8.4 of the same regulation. If the assessment carried out in the SMS Manual addresses the aforementioned minimum aspects, then a cross-reference in the SSA would suffice.

Once the assessment process is completed, the security measures and weaknesses identified in the SSA should be addressed in detail in the SSP[6]. As stated above, cybersecurity should be addressed in the ship's SMS, according to IMO MSC 428 (98). As such, in order to satisfy the requirement of Annex III Paragraph 8.3.5 of Regulation (EC) 725/2004, if the SSP does not include cybersecurity measures in detail, it should, at least, include a cross reference to the relevant section of the SMS (or any other document, e.g. a separate cybersecurity plan), which hitherto, will be considered part of the SSP.

3.1.2. Ship security plan

Preparation of an effective SSP should rest on a thorough assessment of all issues that relate to the security of the ship[7], including cybersecurity.

Therefore, the SSP must include (or reference) measures to address the cybersecurity weaknesses identified in the SSA. These could include procedures for addressing cyber threats and preventing, responding to and recovering from cyber incidents, including provisions for maintaining critical operations of the ship, as identified in the SSA. The minimum set of these measures is described in the following table.

Table 1 Recommended minimum measures for basic cyber hygiene onboard

Control	Description	Inspector activity
Asset Inventory	Establish and maintain an inventory of digital systems onboard the ship. The list, which could be part of the SSA, may be categorised to business, crew, IT, and OT systems.	Check that the list exists. Check last update date. Check that there is a designated individual/s for updating the list.
Update management	Establish and maintain a process for updating and monitoring the versions of IT/OT systems and software onboard the ship.	Check that there is a process for this, and it is stated in the SSP. Check last update date.
Data protection and backup	Establish a process to identify, classify and backup the data handled and stored onboard the ship. This data may include crew sensitive data and operational data.	Check that there is a process. Check that the process is known to the designated individual for cybersecurity. Perform crew interviews to collect evidence. Check if the process is correctly implemented on board.
USB Protection & Removable	Establish controls to protect systems from the use of unauthorised removable media. Minimise the use of external	Check for evidence of physical or digital USB protection (e.g. visible physical blockers or software used for that).

[6] Regulation 725/2004, Annex III, Paragraph 9.1
[7] Regulation 725/2004, Annex III, Paragraph 9.3

device management	removable devices, such as USB sticks and Hard Disc Drives. Protect systems onboard by locking, physically and digitally, USB ports[8].	
Account and access control management	Establish a process to assign, manage and revoke credentials for user accounts linked to crew identity and not positions.	Check that there is a process, list or software for that[9]. Check that the process is known to the designated individual for cybersecurity. Ask for evidence by randomly selecting officers to log in to their accounts.
Network management	The ship network should be segregated to, at least, business and crew. Further segregation between IT and OT systems is desirable[10]. It should be protected with a security technology, such as a firewall.	Check that equipment or software onboard exists for that (e.g. switch or firewall, etc)[11]. Interview the designated individual for cybersecurity.
Remote connection protection	All digital systems and devices onboard a ship that have access to the internet, or the company's intranet should be protected with a security technology, such as firewall or antivirus.	Check that equipment or software onboard exists for that. Perform, where applicable, random checks of systems and cross-check with the asset inventory list.
Cybersecurity awareness and training	Include cybersecurity to crew training, drills, and exercises. Log these activities as required.	Check that crew training certificates are available. Check records where these activities are logged[12].
Incident detection, response, and recovery	Include cybersecurity related incidents in the existing security detection, response, recovery and reporting procedures.	Check that there is an incident response plan dedicated for cybersecurity or which includes cybersecurity. Check that the plan includes detection and reporting procedures. Ask for evidence by randomly interviewing crew members on the existence and content of the plan. Check logs of when recovery process was last tested.

This non-exhaustive list of controls aims to address several aspects when considering cybersecurity. In general, these may include the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data, as well as the safety, trustworthiness,

[8] Physical and logical control rules and configuration can be displayed. For physical control, usage of port lockers can be a way, and for logical, rules in the system registry can be presented (whitelisting/blacklisting).

[9] If software is used ask for vendor/version.

[10] In the case of passenger ships, passenger service networks must be segregated from the rest and duly protected.

[11] For checking that a proper network segmentation is established, firewall configuration rules and IP tables can be presented as evidence.

[12] Training plan traceable through a logbook (paper or digital).

resilience, and control of all software enabled systems and equipment onboard the ship. **These set of controls are the minimum elements that should be checked in any activity (audit, control, verification, inspection) that has a cybersecurity component.**

For that purpose, a checklist that can be used by inspectors, auditors, and surveyors is included in Annex A.

3.2. Annex III, Para. 9.2 Reg 725/2004: Components of a Ship Security Plan

3.2.1. Security organisation of the ship[13]

The SSP (or the equivalent reference document) should describe the roles and responsibilities of cybersecurity personnel for the ship, including how and when physical security and cybersecurity personnel onboard and ashore will coordinate activities and conduct notifications for suspicious activity, breaches of security, or heightened security levels.

3.2.2. Links with other authorities[14]

The SSP (or the equivalent reference document) should detail the ship's links with other relevant authorities, in particular here, cybersecurity authorities (e.g. national cybersecurity authority or cybersecurity incident response centres) that it may need to contact in case of a cyber incident, threat or suspicious activity. Due to the nature of information that will have to be shared in such a case, this link may be done through the shipping company's competent personnel.

3.2.3. Communication systems

The SSP (or the equivalent reference document) should detail the necessary communication systems to allow the effective continuous operation of the ship and its links with others, including port facilities[15]. To the extent that software enabled systems are used to perform this function, the SSP may describe how those systems are protected, include an approved and secure alternative means of communication, and detail the personnel communication responsibilities should the system be compromised or degraded.

3.2.4. Security levels

The SSP should detail if additional cybersecurity measures are to be put in place at security level 2 and/or 3[16]. For example, additional readiness to switch from main to alternative systems or digital to paper-based operations.

[13] Regulation 725/2004, Annex III, Paragraph 9.2.1
[14] Regulation 725/2004, Annex III, Paragraph 9.2.2
[15] Regulation 725/2004, Annex III, Paragraph 9.2.3
[16] Regulation 725/2004, Annex III, Paragraph 16.3.4

3.2.5. Reporting security incidents

The SSP (or the equivalent reference document) should address the procedures for detecting and reporting a cybersecurity incident, as any other security incident[17].

According to Regulation 725/2004, a "security incident" means any suspicious act or circumstance threatening the security of a ship[18]. In this context, a "cybersecurity incident" that should be reported is an incident that compromises the functioning of operations in the ship, such as cargo handling equipment or loading and stability computers, GMDSS/GNSS or leads to compromise of data handled by the ship's network and information systems. Failed or countered cyber incidents that would otherwise have had such consequences should also be reported. Incidents that could also be reported which may not systematically have direct and obvious impact on the ship operations include repeated phishing emails, suspicious emails, unusual functioning of computer systems or networks.

The SSP (or the equivalent reference document) should indicate the authority to which a cyber incident is reported. If a cyber incident is reported to a national authority competent for cybersecurity, the national authority competent for maritime security should also be informed, and vice versa. This should be done by either the ship or shipping company, or by the cybersecurity national authority, depending on how the Member State wishes to organise this.

Records of cybersecurity incidents should be kept. The analysis of the cyber incidents that occurred should be part of the SSA review, in order to evaluate the effectiveness of existing counter measures and establish proper ones to mitigate the emerging vulnerabilities.

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.

3.2.6. Training, drills and exercises

As drills should test individual elements of the SSP[19], if cybersecurity measures are included in the SSP, then some drills may focus on readiness against cyber incidents and the personnel's knowledge of cybersecurity.

As exercises should test communication, coordination, resources availability and response, if cybersecurity measures are included in the SSP, then some exercises may focus on testing the effectiveness of communication and coordination among crew, shipping company, IT department and Competent Authority, in case of a cybersecurity incident.

If cybersecurity is addressed in another document, i.e. the SMS manual, drills and exercises should be carried out in accordance with instructions laid out in that document. In any case, cybersecurity drills and exercises are counted as security drills and exercises, as outlined in Regulation (EC) 725/2004.

[17] Regulation 725/2004, Annex II, Paragraph 9.4.12
[18] Regulation 725/2004, Annex I, Regulation 1, Paragraph 1.13
[19] Regulation 725/2004, Annex III, Paragraph 13.5

These 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 incident.

3.2.7. Documentation and records

Electronic records should be protected against unauthorized deletion, destruction, or amendment. If the SSP is kept in electronic format, then it must be protected by procedures aimed at preventing its unauthorised deletion, destruction, or amendment[20].

4. Port State Control Inspections and Cybersecurity

The Paris MoU instruction 54/2021/02 provides guidelines for PSC Officers with regards to ISPS requirements, while instruction PSCC 55/2022/09 provides guidelines on the ISM Code. This latest Instruction states that "ISM auditing is the responsibility of the flag State and the Company and does not fall under the scope of port State control".

Therefore, a PSC officer, qualified as DAO, conducting a PSC inspection cannot perform an audit of the ISM safety management system, where cybersecurity procedures on board the ship could be included. However, if, during a PSC inspection, the PSC Officer/DAO conducting the inspection has clear grounds for believing that the ship is not in compliance with the requirements of the special measures to enhance maritime security of the SOLAS Convention and of the ISPS Code (e.g., passwords noted on post-its, attached to the automation screens in the ship's ECR), he/she could evaluate to carry out a DAO inspection (or to refer to the MARSEC competent authority), pursuant art. 8 of Regulation (EC). 725/2004. Regarding cybersecurity, this could only happen in an EU port for EU Member State flagged ships, considering that the para. B/8.3.5 of ISPS is only mandatory under EU legislation.

It is clear that the cybersecurity procedures, indicated in the SMS manual, could be verified during a flag State inspection, for which the limitations envisaged for the PSC domain, are not applicable.

5. Conclusion

With cybersecurity increasingly being a challenge for the maritime sector, including ships, the European Commission wishes to clarify the relevant provisions of EU maritime security legislation in this regard, in order to implement a standardized and harmonized approach for ships operating under an EU Flag. As maritime and cybersecurity practices evolve with time, this guidance may be updated whenever deemed appropriate.

[20] Regulation 725/2004, Annex II, Paragraph 9.6

Annex A: Checklist for maritime security inspectors, auditors, and surveyors on cybersecurity onboard ships

Control	Question/s	Response	Comments
Asset Inventory	1. Is there an asset inventory in place for all IT and OT systems/devices onboard? 2. Is there a procedure in place for updating this and adding any new equipment as soon as it is installed?	Y/N Y/N	
Update management	1. Is there a process for updating and monitoring the versions of IT/OT systems and software onboard the ship? If so, is this stated in the SSP/any other relevant document? 2. Is there a designated individual to monitor this process, onboard or ashore?	Y/N Y/N	
Data protection and backup	1. Is there a process in place to identify, classify and backup the data handled and stored onboard the ship? 2. Is there a designated individual to monitor this process?	Y/N Y/N	
USB Protection & Removable device management	1. Are USB ports on all devices onboard protected with a physical and/or digital lock? 2. Are there controls (physical and digital) in place to protect systems from the use of unauthorised removable media? If so, which are these controls?	Y/N Y/N	
Account and access control management	1. Is there a process and/or software for assigning, managing and revoking credentials for user accounts? 2. Are credentials for user accounts linked to crew identity and not positions?	Y/N Y/N	
Network management	1. Are onboard networks segregated? If so, evidence should be provided to illustrate the network architecture. 2. Are networks onboard protected with at least one security technology (e.g. switch, firewall, etc)?	Y/N Y/N	
Remote connection protection	1. Are all systems with a remote connection (e.g. access to the internet the company's intranet, etc.) included in the asset inventory list?	Y/N	

	2. Are these systems protected with at least one security technology (e.g. firewall, antivirus, IDS, IPS[21], etc.)	Y/N
Cybersecurity awareness and training	1. Is cybersecurity included in the crew training planning?	Y/N
	2. Are records of crew cybersecurity training kept onboard?	Y/N
	3. Does the crew know who the designated person for cybersecurity is onboard?	Y/N
Incident detection, response, and recovery	1. Is there an incident response plan dedicated for cybersecurity or which includes cybersecurity?	Y/N
	2. Are reporting procedures of a potential cyber incident included in the incident response plan?	Y/N
	3. Is the crew aware of the reporting procedures and initial actions in case of detection of a potential cyber incident?	Y/N

[21] IDS: Intrusion Detection Systems, IPS: Intrusion Prevention Systems

References - Relevant documents

1. Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security

2. Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC

3. Regulation (EC) No 336/2006 of the European Parliament and of the Council of 15 February 2006 on the implementation of the International Safety Management Code within the Community

4. Directive 2009/16/EC of the European Parliament and of the Council of 23 April 2009 on port State control, as amended

5. IMO MSC 428 (98) “Maritime Cyber Risk Management in Safety Management Systems” and other relevant IMO documentation

6. IACS UR E26

7. IACS UR E27

8. The Guidelines on Cyber Security onboard Ships - Version 4 (BIMCO et al)

9. US Coast Guard Navigation and Vessel Inspection Circular (NVIC) 1-20, “Guidelines for addressing cyber risks at Maritime Transportation Security Act (MTSA) regulated facilities”, 26 February 2020 and other relevant USCG documentation