Council of the European Union

Brussels, 22 February 2016
(OR. en)

6384/16

OMI 22
MAR 58

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	22 February 2016
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2016) 40 final
Subject:	COMMISSION STAFF WORKING DOCUMENT For the Council Shipping Working party IMO – Union submission to be submitted to the 96th session of the Committee on Maritime Safety (MSC96) of the IMO in London from 11 – 20 May 2016 concerning measures aimed at improving cybersecurity on a ship

Delegations will find attached document SWD(2016) 40 final.

Encl.: SWD(2016) 40 final

EUROPEAN
COMMISSION

Brussels, 22.2.2016
SWD(2016) 40 final

COMMISSION STAFF WORKING DOCUMENT

For the Council Shipping Working party

IMO – Union submission to be submitted to the 96th session of the Committee on Maritime Safety (MSC96) of the IMO in London from 11 – 20 May 2016 concerning measures aimed at improving cybersecurity on a ship

COMMISSION STAFF WORKING DOCUMENT
For the Council Shipping Working party

IMO – Union submission to be submitted to the 96th session of the Committee on Maritime Safety (MSC96) of the IMO in London from 11 – 20 May 2016 concerning measures aimed at improving cybersecurity on a ship

PURPOSE

The document in Annex contains draft a draft Union submission to the 96th session of the Committee on Maritime Safety (MSC96) of the IMO. It is hereby submitted to the appropriate technical body of the Council with a view to achieving agreement on transmission of the documents to the IMO prior to the required deadline of 8 March 2016[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 and Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security implements the maritime security regime agreed by the International Maritime Organization (IMO) in December 2002 in SOLAS chapter XI-2 and the International Ship and Port Facility Security (ISPS) Code. In particular Article 3(5) of Regulation (EC) No 725/2004 renders some provisions of Part B of the ISPS Code mandatory, including the minimum standards for Ship Security Assessment (SSA).

Compliance with the ISM Code is regulated at EU level through Regulation (EC) No 336/2006 on the implementation of the International Safety Management Code within the Community and repealing Council Regulation (EC) No 3051/95.

[1] The submission of proposals or information papers to the IMO, on issues falling under external exclusive EU competence, are acts of external representation. Such submissions are to be made by an EU actor who can represent the Union externally under the Treaty, which for non-CFSP (Common Foreign and Security Policy) issues is the Commission or the EU Delegation in accordance with Article 17(1) TEU and Article 221 TFEU. IMO internal rules make such an arrangement absolutely possible as regards existing agenda and work programme items. This way of proceeding is in line with the General Arrangements for EU statements in multilateral organisations endorsed by COREPER on 24 October 2011.

Furthermore, the Commission's proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union[2], establishes security requirements also for market operators with a view to achieving the scope of ensuring a high common level of network and information security. In this context market operators include maritime carriers. Therefore, the substance of the draft Union submission falls under EU exclusive competence.

ANNEX

MARITIME SECURITY COMMITTEE
96th session
Agenda Item 4

MSC/96/4/xx.
March 2016
Original: ENGLISH

Measures aimed at improving cybersecurity on a ship

Submitted by the European Commission on behalf of the European Union

SUMMARY

Abstract:	The purpose of this document is to contribute to the implementation of appropriate measures on a ship to cope with an attack on its information system. This threat is addressed through three measures, following an analysis to improve cybersecurity on board a ship.
Strategic orientation:	6.1
High-level measure:	6.1.1
Expected results:	6.1.1.2
Measures to take:	Paragraph 16
Reference documents:	MSC 95/22 – MSC 94/4/1 – MSC 96/INFXX

[2] COM/2013/048 final.

Introduction

1. During the 95th session of the Maritime Security Committee, the Committee asked member States and international organizations to collaborate on the subject of proposals for recommendations for maritime cybersecurity, and to submit them to MSC 96 (MSC 95/22 para 4.13). This document aims at contributing to an improvement of the Information Security Systems (ISS, including information technology (IT) and operational technology (OT)) on board a ship.

2. The sea is an essential and unavoidable medium of international trade. The large number of players in this trade increases vulnerability to security threats. Up to now, the standards, methodologies and tools dedicated to the analysis and detection of these security threats have been monolithic and focus only on physical security. These major principles are based on the ISPS Code. In this context of protection of trade, the digital domain has been progressing constantly since the beginning of the nineties. This domain is now omnipresent in the management of shipping and port activities. It now seems impossible to do away with this technology, which regulates the communications systems and control systems of a sea vessel.

3. Now the domain of attacking digital systems has become a realm of action for isolated groups or criminal groups. The maritime world is no longer free from these malicious attacks, which can be intended to destabilize, spy, sabotage and, in some circumstances, commit cybercrime (with ransomware and phishing), as was reiterated by the United States and Canada in document MSC.94/4/1. Thus, it seems essential to prepare ships for this threat. This form of protection is referred to as "cybersecurity". "Cybersecurity" is defined as the range of information technology processes intended to protect data being transmitted over the Internet, and to combat the threat of the installation of malware programs.

4. For some years, the possibility of a threat in the management of the digitization of data in a port or on a ship has been known. To counter this, e.g. France has the Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), or National Information Systems Security Agency.

5. Also e.g. in France, a workgroup on cybersecurity on board a ship has been founded. Since June 2015, the workgroup has established 3 lines of work:

- Review the state of the art in IT data protection on board ships under the French flag. This review formally consisted of a one-year survey on board ships under the French flag, to evaluate the degree of recognition of this threat.
- Perform a security audit of the information system on board a sensitive and complex vessel. This audit aims to evaluate the measures to be improved to counter this type of threat.
- Produce an information guide on best information technology practices, intended for all crew members on board a ship under the French flag.

Discussion

6. To date, only the ISPS Code lays down a regulatory specification for the management of information technology processes. This code states that the vulnerability of the information system must be evaluated (Ship Security Assessment) from the viewpoint of the vessel's security, so as to be availed of appropriate measures for whatever threat. To augment this, it seems essential to undertake a nationwide review of the management of information technology protection systems on board ships.

7. In view of this, e.g. in France a survey has been underway since August 1, 2015, on board ships under the French flag. This survey aims to define the degree of protection of a ship's information systems. The methodology and analysis are described in MSC96/INFXX.

8. As a complement to this survey, an ISS audit was conducted on board a ro-ro passenger ship. The purpose and method of this audit are described in the second paragraph of the MSC96/INFXX document.

9. The third phase of analysis concerning the approach to this threat on board a ship consists in raising the vessel's crew's awareness about cybersecurity. This stage involves the production of a best practices guide for use aboard ships. The guide is currently being proofread before distribution to ship owners. The guide is a simple approach, and is intended to teach everyone on board the ship some elementary habits in terms of information technology security. The guide contains the following sections:

- Choosing your passwords with care;
- Being careful when using one's email/messaging;
- Separating personal use from professional use;
- Being careful on the Internet;
- Taking regular backups;
- Properly knowing your users and service providers;
- Regularly updating your software;
- Downloading your software from software developers' official sites;
- Securing the vessel's WiFi access;
- Other advice: Smartphones, travel,

Protective measures appropriate for the vessel

10. To protect the vessel, it is important to define the following concepts:

- Networks: uncontrolled networks are not under a security surveillance system on board the ship;
- Critical networks: networks used for navigation, propulsion, energy management on board the ship, cargo management, passenger management, alarm management, and the administrative management of the vessel are classified as critical;
- Network access: The workstations are multi-user and are accessible by function,
- ISS best practices**:** This domain covers access management and the updating and backing-up of the vessel's information system.

11. At the present time, standards address the domain of information security by proposing a governance model through the standard ISO/IEC 27001 and the associated certification. In the "2700x family" of standards, there is the concept of "information Security Management System". It is important to say that the standard targets the implementation of a process, and does not impose a minimum security level. It principally involves saying what will be done (draft a policy, an action plan), doing what has been said ("do" actions implemented), checking what has been done ("check" internal audit), and correcting and improving over time ("act" experience feedback). This philosophy has already been adapted to ships through International Safety Management code (ISM).

12. The tools to be employed for information security protection on board a ship are of two kinds: management tools and technological tools.

- **Management tools onboard a ship:** Management of a vessel in safety and security terms is based on the ISM and ISPS certification. The Safety Management System includes references to the security of on board information systems, with reference to these two codes. However, these references to information security or information technology security are generally very rudimentary. For its part, the Ship Security Plan provides a purely-physical approach to the security of on board information systems. The Ship Security Plan and the Safety Management System are the appropriate documents to contain references to the ship's and the company's cybersecurity policies.

- **Technological tools:** Data protection on board a merchant vessel does not demand an approach on the same level as that required for a research laboratory. Therefore, an effective cyber-protection strategy employs simple and inexpensive commercially-available means. The technological tools to be deployed are the following:

    1. Antivirus: system "prerequisite".
    2. Firewall: activate and configure the computer's ports so as to organize and interchange data through ports. Prevent a software program from being able to test whether a port is "open" or not. The first tool that a pirate has is a software program that scans all the ports of a list of IP addresses having been selected or chosen randomly to detect "potential targets". If all the "ports" are closed, the IP scanned will be skipped and the program will proceed on to another IP to test. Therefore, the computer is "invisible" to pirates.
    3. **VPN** (Virtual Private Network): a VPN link is also referred to as a "tunnel", because the image aptly describes what a VPN does: it creates an encoded envelope for all the information that transits through it, making data unreadable and thus unusable for any external interception. Only the end points of the tunnel (the computers) can encode/decode the data interchanged. The other additional advantage of a VPN is that it "conceals" the IP of the connected computers, and replaces them with those of the intermediary servers (which know the real IPs but keep them encoded).
    4. **Anti-spyware**: certain spy programs are not considered to be viruses and therefore successfully pass through the antivirus. Therefore, an association of 2 types of program are needed for proper protection.
    5. **Sandbox**: a "sandbox" is a technology offered by certain antivirus products, or by dedicated software products. This creates a totally sealed space from which neither viruses nor spyware nor malware can escape to reach the host computer. Before opening an unknown or untrustworthy Web page, the sandbox is opened and then the untrustworthy Web page is opened in the sandbox's Web browser.
    6. **Message and WiFi encryption software**: some websites offer this service free-of-charge or at a small price. An encrypted email is unreadable even if it is intercepted.
    7. **IDS (Intrusion Detection System)**: such a system detects any intrusion.
    8. **NAS (Network Attached Storage):** this is an autonomous file server connected to a network of which the main function is data storage in a centralized repository for network clients.

13. To cope with the threat of a malicious act on a ship's information system, France has drafted an initial guide that is based on a set of 7 sheets and an analysis of the objectives to be accomplished. This guide is described in Appendix C of MSC96/INFXX.

14. Guidelines to be envisioned in the short-term: The vessel's access management procedure already provides physical protection against unintended access to a ship's information systems. Access to these systems must now be constrained and regulated.

The stipulations of the ISPS and ISM Codes enable a fast roll-out of a framework for handling the management of information system security on board a ship. The principal advantage of this solution is that it is not necessary to create a new system. One simply needs to adapt the "tools" used in the maritime world. Providing appropriate ISS protection for a ship involves the following 9 aspects:

N° 1	Do an assessment of the ship's Information Security Systems (ISS including Information technology (IT) and operational technology (OT))	Code ISPS B8.3
N° 2	Apply the physical protection measures for the ship's information systems (priority is given to the restricted areas of the ship).	Code ISPS A9.4.2
N° 3	Draft a company information systems policy for the ship.	ISM code, chap1
N° 4	Train the crew on the ship's information systems.	ISM code, chap 6
N° 5	Apply best practices in management of information systems on board the ship,	ISM code, chap7
N° 6	Apply checking on interchanges by the information systems on board the ship,	ISM code, chap7
N° 7	Implement an operational continuity plan for after an incident.	ISM code, chap 8
N° 8	Manage the ship's information systems incidents.	ISM code, chap 9
N° 9	Implement checking of activity of the ship's information systems.	ISM code, chap 12

15. Guidelines to be envisioned in the short-term: Technological solutions exist that can be adapted to the vulnerabilities and needs of a ship. The ISS evaluation is the basis for any action to be taken on board a ship. Sheets 1 to 7 of Appendix C of the MSC 96/INFXX document list the tools that can be installed, according to the vessel's needs.

Additionally, several measures would contribute to a better coverage of cyberattack prevention:

- Have a printer external to all networks, that is available to all parties external to the ship: agent, port state control, flag state control. This basic precaution prevents any outside infections and enables the vessel's administrative networks to be isolated.

- Restrict WiFi connections during the ship's sensitive operations (vessel approach, and cargo management).

- Impose the standard IEC 61162-460 (MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security) for new vessels.

Proposal

16. It is proposed that a guide should be drafted by the Committee to enable companies to better cope with an act of cyber criminality, drawing inspiration from Appendixes C, D, E of MSC96/INFXX.

Action requested of the Committee

17. The Committee is invited to take note of the proposal in paragraph 16 and take action as appropriate.