DRAFT II

DRAFT FOR COMMENTS

Subject: Inclusion of Cyber Security measures in Ship Security Plan - reg.

1. One of the objectives of ISPS code is to take preventive measures against security incidents affecting ships and ports.

2. Cyber security may affect the safety and security of ships. In view of the same, efforts need to be taken to enhance cyber security on ships.

3. In view of the progress of Information Technology, day-to-day ship operations have become increasingly dependent upon the use of such technology. Due to the inherent interconnected nature of such activities attack on this infrastructure can adversely affect ship operations.

4. Cyber security is therefore necessary for the maintenance of integrity and availability of information and systems, ensuring continuity of businesses with secure utilization of digital assets and systems.

5. Cyber systems are generally categorized as Information technology (IT) system and Operational Technology (OT) system. IT system manages the flow of information and data computation. In contrast, OT system manages the operation of the physical processes and equipment.

6. The increasing role of IT and OT system on board ships and in ports/ marine infrastructure exposes such system to risk of malicious attacks or unauthorized access which may directly impact security and safety of the ship and its surroundings areas.

7. The implication of a cyber-attack may range from loss of data, compromise of system and possible loss of life or platforms in extreme situations.

8. Several aspects can affect cyber security on ships. Some of them are:

- Confidentiality : The ship system and associated processes should be designed, implemented, operated and maintained so as to prevent unauthorized access to for example, sensitive, financial, security, commercial or personal data.
- Possession and/or control: The ship systems and associated processes should be designed, implemented, operated and maintained so as to prevent unauthorized control, manipulation or interference.
- Integrity: The ship systems and associated processes should be designed, implemented, operated and maintained so as to prevent unauthorized changes being made to assets processes, system state or the configuration of the system itself.
- Authenticity: Ensuring that inputs to and outputs from, ship systems, the state of the systems and any associated processes and ship data are genuine and have not been tempered with or modified.
- Availability: Ensuring that the asset information, systems and associated processes are consistently accessible and usable in an appropriate and timely fashion.
- Utility: The ship systems and associated processes should be designed, implemented, operated and maintained so that the use of ship assets is maintained throughout their lifecycle.
- Safety: The design, implementation, operation and maintenance of ship system and related processes so as to prevent the creation of harmful states which may lead to injury or loss of life, or unintentional physical or environmental damage.
- Resilience: The design, implementation, operation and maintenance of ship systems and associated processes should be such that cascade failures are avoided.

9. To improve cyber security, it needs to be ensured that the shipboard design of the systems as well as shore based system design and their associated processes are resilient and that appropriate alternatives are available in case of compromise to the system. Personnel security aspects may also need to be factored.

10. In view of the foregoing and the importance of cyber security measures to ensure continued safety and securely on ships, the cyber security measures of ships are to be included in Ship Security Assessment (SSA) and thereafter in the Ship Security Plan (SSP) of every Indian Ship.

11. The Master and Ship Security Officer (SSO) should have reasonable knowledge of cyber security aspects and the company may consider such officers to undergo a suitable training on cyber security measures so as to be able to deal with cyber security threats.

12. While carrying out assessment of cyber security threat should identify and document the following needs to be carefully evaluated

a) Cyber Physical System (CPS)

b) Sensitive Ship Systems (SSS)

c) The Security Sensitive Information (SSI)

Note:

a) Cyber Physical System (CPS) is a system designed as an entity or set of entities, with a specific purpose, or to meet a capability objective. A CPS should include a computational aspect (cyber) and a physical aspect working together to accomplish a task or function. (Example, the automated steering of a ship to maintain a planned course).

b) Sensitive Ship Systems (SSS) are assets, which as a whole, or in part may be of interest to anyone for hostile, malicious, fraudulent and/or criminal or activities.

Such systems will vary according to the type and function of a ship, but are likely to include:

a. critical systems;
b. systems required for the safety of life and safe operation of the vessel;
c. systems holding personal information;
d. VDR.

Access to such systems should only be allowed to relevant authorized personnel only.

c) Security Sensitive Information (SSI) is SSI is information the disclosure of which will compromise the security of the ship, including, but not limited to, ship operational data, or privileged or confidential information that would compromise any person, system or an organization.

13. Every Indian Ship is advised to carry out assessment of cyber security system and may consider incorporating the same in the SSP. The critical areas such as server room, areas with computer access etc. may need to be included in restricted areas. Access control to such areas may also need to be reviewed and revised.

14. This is issued with the approval of the Nautical Adviser to Govt. of India (i/c).

(Capt. Nitin Mukesh)
Nautical Surveyor-cum-Dy. Director General (Tech)