Director General of shipping, Ministry of Shipping, Govt. of India, Mumbai		
Authorized by the Chief Surveyor with GOI	**ISM CELL**	**ENGG. Circular No.06 of 2017**
	Subject: Implementation of Cyber-security risk mitigation measures on board Indian Flag Ships	
	File No. : ENG/ISM-59(4)/97-Vol VII.	**Dated: 06.11.2017**

A) Back ground:

1) Modern developments in information and communication technology have led shipboard machineries and equipments fitted with complex control systems and such control systems are increasingly being networked with the information technology wherein the technology uses data as information for operation, monitor and control the physical processes.

2) The exchange of information and data via networked systems using internet is susceptible to cyber-attack. The consequences of a cyber-attack are wide-ranging, that is, from business disruption, damage to ship, pollution, safety of crew to ship collision. Therefore, it is important that these information and data exchange systems be protected from risks that may occur via un-authorized access or malicious attacks to ships' systems and networks and from personnel having access to the systems onboard, for example by introducing malware via removable media.

3) To address the issues related to cyber-security IMO at the 98th session of the Maritime Safety Committee held on June 16, 2017, approved Resolution MSC.428 (98) on *Maritime Cyber Risk Management in Safety Management Systems.* The resolution affirms that approved safety management systems should take cyber risk management into account in accordance with the objectives and requirements of the International Safety Management Code. Further the member states are encouraged to ensure cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

4) The IMO guidelines define cyber risk management as being "the process of identifying, analyzing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating [that risk] to an acceptable level [after] considering the costs and benefits of actions taken to stakeholders." Further, Cyber risk management should be considered a part of operational risks and should evolve "as a natural extension of existing safety and security management practices".

Ramesh 6/11/2017.

B) Requirements:

1) To ensure that **all shipping companies holding DOC** issued under ISM Code comply with the IMO requirement within the prescribed time limit, the Directorate hereby specifies the following procedure:

i) All new DOC applicants requesting for initial DOC audit on/after 1 January 2018:

a) Cyber-risk management procedures to be included in the SMS risk mitigation manuals. These procedures to be reviewed by Recognized Organization prior conduct of initial DOC audit by the Administration auditor.

b) Review and verification of satisfactory implementation of the said cyber-security risk mitigation during the initial audit by the Administration Surveyor. The initial audit report narrative and Document review record narrative to clearly state the same.

c) A suitable memo (stating the satisfactory compliance to the said IMO requirement) be raised in the survey status of each vessel owned/managed by the said company by the RO conducting the initial audit after satisfactory verification of the implementation of the cyber-risk mitigation measure on board each such vessel during the initial audit. The audit report narrative to include verification of the compliance with such requirement on board.

ii) All other existing DOC holders wishing to demonstrate compliance prior to 1st January 2018:

a) It is advised that Indian DOC holders may not wait till the 1st annual/renewal DOC audit after 1st January 2021.

b) A Company wishing to demonstrate compliance with the said IMO requirement earlier may carry out a cyber-risk assessment and include the mitigation procedures in their SMS after due review by RO.

c) Request DGS auditor to verify compliance during the next due annual/renewal DOC audit. Administration auditor to follow procedures detailed in Paragraph B)1(i)(b) above with respect to verification and reporting during this annual/renewal DOC audit. A copy of such report to be forwarded by the Company to the concerned RO/s which conducted previous SMS audits on the Company managed vessels.

d) RO/Administration auditor carrying out the next due intermediate/renewal SMS audit (after demonstrating the verification of compliance in the last DOC audit)on the Company managed vessel/s to follow procedures detailed in Paragraph B)1(i)(c) above with respect to compliance, report narrative and raising of a suitable Memo in the survey status of the said vessel/s.

Ganesh
6/11/2017.

iii) **On/After 1 January 2021:**

a) No request for DOC annual/renewal audit shall be accepted unless risk mitigation procedures reviewed by RO are included in the SMS manuals.

b) No request for vessel/s SMC intermediate/renewal audit shall be entertained unless the report narrative of previous DOC audit states compliance with the said IMO requirement with respect to cyber-security risk management.

This is issued with the approval of the competent authority.

6/11/2017.

(Satish Kamath)

Engineer and Ship Surveyor-cum-Dy.Director General (Tech)

To,

1. The Principal Officer/ Mercantile Marine Department, Mumbai/Kolkata/ Chennai/ Kandla/Cochin.
2. The Surveyor-in-charge, Mercantile Marine Department, Goa/Jamnagar/Port Blair /Visakhapatanam /Tuticorin /Delhi /Haldia/ Paradip /Mangalore.
3. All Recognised Organizations.
4. ICC Shipping Association (ICCSA), Mumbai.
5. CS/NA/CSS/Jt.D-G.
6. Hindi Cell.
7. Guard file.
8. Computer Cell.