C C S Technical Information

(2020) Technical Information No.68 Total No.502
Nov.30,2020
(Total 2 pages)

To: All CCS branch offices, CCS auditor, Shipping companies.

Technical notice on the vessel cyber risk management work instruction released by USCG

USCG released vessel cyber risk management work instruction on October 27,2020. This work instruction (WI) provides guidance regarding the U.S. Coast Guard (USCG) commercial vessel compliance program's approach to assessing the cyber risk on vessels to ensure vessels do not pose a risk to the Marine Transportation System (MTS) due to a cyber event. To push the implementation of the resolution MSC.428(98) as soon as possible, all parties concerned are reminded of paying attention to this WI and the followings:

1. As the requirements of the resolution MSC.428(98), 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. USCG will start the vessel compliance activities after 1 January 2021 accordingly.

2. The PSCO shall identify when basic cyber hygiene procedures are not in place onboard. These include, but not limited to the following:

a. Poor cyber hygiene

1) Username / Password openly displayed

2) Computer system appears to require a generic login or no login for access

3) Computer system does not appear to automatically log out after extended period of user inactivity

4) Heavy reliance on flash drive/USB media use

b. Shipboard computers readily appear to have been compromised by ransomware/excessive pop-ups

c. Officers/crew complain about unusual network issues and reliability impacting shipboard systems

d. Unit/vessel screener received potential 'spoofed' email from master/crew onboard.

3. USCG vessel compliance activities are only directed towards cyber risk

management on systems that are critical to the safe operation and navigation of the vessel. Stand-alone computers or other systems which do not affect the safe operation or navigation of the vessel are not to be inspected or examined. If the above observations are not directly linked to statutory requirements or are not technical or operational-related deficiencies, the PSCO does not have clear grounds to conduct a more detailed inspection.

4. If objective evidence is identified indicating that the vessel failed to implement its SMS with respect to cyber risk management, the PSCO shall direct the vessel to take the following actions:

1) If cyber risk management has not been incorporated into the vessel's SMS by the company's first annual verification of the DOC after January 1, 2021, a deficiency should be issued with action code 30 – Ship Detained, with the requirement of an external audit within 3 months or prior to returning to a U.S. port after sailing foreign.

2) When objective evidence indicates that the vessel failed to implement its SMS with respect to cyber risk management, then the PSCO shall issue a deficiency for both the operational deficiency and an ISM deficiency with an action code 17 – Rectify Prior to Departure and require the vessel to conduct an internal audit, focused on the vessel's cyber risk management, within 3 months or, prior to returning to a U.S. port after sailing foreign.

3) When objective evidence indicates there is a serious failure to implement the SMS with respect to cyber risk management that directly resulted in a cybersecurity incident impacting ship operations (e.g. diminished vessel safety/security, or posed increased risk to the environment), after gaining concurrence from the OCMI, the PSCO shall issue a deficiency for both the operational deficiency and an ISM deficiency with action code 30 –Ship Detained with the requirement of an external audit within 3 months or prior to returning to a U.S. port after sailing foreign.

5.Kindly remind the relevant shipping companies pay full attention of the implementation of MSC.428(98), and address cyber risks in safety management systems as soon as possible. CCS auditor should refer to the USCG' approach when conduct DOC/SMC audit.

6. Please find the attached flag states requirements on maritime cyber risk management from Singapore, Panama, Marshall Island, Liberia for reference.

The Technical Notice is made public on CCS website（www.ccs.org.cn）and is to be forwarded by CCS branches to relevant shipping companies.

Please contact Classed Ship in Service Department of CCS Headquarters in case of any unclarity during the implementation of this Technical Information.
E-mail: cdwork@ccs.org.cn.