PSC Related Circular

No.PSC 20/2020

Dated: 17.11.2020

Subject:

USCG & CYBER SECURITY

USCG has released a new work instruction (CVC-WI-027) to provide guidance to Coast Guard Marine Inspectors and Port State Control Officers for **assessing cyber hygiene onboard** applicable vessels, as well as compliance options if deficiencies are noted.

According to this WI, the USCG expects that all companies with U.S. flagged vessels and **foreign flagged vessels that call on ports in the U.S. should ensure cyber risk management is appropriately addressed in their SMS.**

If objective evidence is identified indicating that the foreign flagged vessel that calls on ports in the U.S. failed to implement its SMS with respect to cyber risk management, the following actions should be directed by the PSCO:

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.**
2) When objective evidence indicates that the **vessel failed to implement its SMS with respect to cyber risk management**, a **deficiency** for both the operational deficiency and an ISM deficiency should be issued with an **action code 17 - Rectify Prior to Departure** or an action code 30 – Ship Detained depending on its seriousness.

WHAT ARE THE USCG LOOKING FOR WHEN THEY INSPECT A SHIP/ UNIT?

Ideally, they will find a vessel that has fully integrated cyber risk management into its SMS, and has ample documentary evidence to prove it. However they have been tasked **to look out for evidence of poor cyber hygiene problems, including but not limited to the following**:

A. **Poor cyber hygiene** (such as password and/or logins on open display, generic logins or no logins, no automatic logout after a period of inactivity, heavy reliance on USB drives and no obvious means of virus checking prior to use)

B. Evidence of **malware on ship computers** – popups /**any ransomware**

C. Records or complaints of **unusual network activity** / reliability issues impacting shipboard systems

D. Spoofed/**phishing e-mails** purporting to come from skipper/crewmembers

Owners are reminded of the **eight critical systems** within the ship: **ballast control**, **engine & propulsion control**, **rudder control**, **cargo control**, navigation (**ECDIS /GPS**), **radar**, **satellite** & **3/4/5G** comms, and on-board **welfare systems**.

Most critically, if the MI/PSCO find a deficiency that has been poorly handled or as a result they are able to conclude that the vessel no longer complies with SOLAS and is therefore unseaworthy, she is likely to be detained.

Example.

The following example is given from the CVC-WI-027, which is self understood and illuminating:

Example: While aboard a ship for a PSC exam the 2nd Officer explains that the ECDIS is not operational after a recent electronic chart update. The PSCO asks the 2nd Officer what is the procedure to update the ECDIS? The 2nd Officer explains that the ECDIS is updated via a flash drive loaded with updates from a shipboard computer (this scenario continues throughout the work instruction).

The PSCO continues by querying the 2nd Officer if the flash drive was scanned for viruses/malware prior to connecting to the ECDIS, and they state "no." At this point, poor cyber hygiene may have occurred and the PSCO has established clear grounds to conduct a more detail exam including the cyber risk management portion of the SMS.

The PSCO reviews the cyber security portion of the vessel's SMS. The SMS requires all thumb drives to be scanned for malware prior to connection to a ship's computer/system. Since the 2nd Officer has already stated that the thumb drive was not scanned, there exists an ISM deficiency.

As a reminder, **cyber risk management must be implemented** into vessel **safety management systems** by the first International Safety Management (ISM) Document of Compliance **verification after January 1, 2021**, in accordance with Maritime Safety Committee Resolution 428(98), "Maritime Cyber Risk Management in Safety Management Systems."

The USCG also issued a Marine Safety Information Bulletin (MSIB 18-20) earlier this year as an advisory on the urgent need to protect operational technologies and control systems.

Finally, the USCG issued MSIB 19-20, to highlight several recent cyber events involving increasingly sophisticated malicious email spoofing techniques within the Marine Transportation System (MTS).

References

- CVC-WI-027: Vessel Cyber Risk Management Work Instruction
- MSIB 18-20: Urgent Need to Protect Operational Technologies and Control Systems
- MSIB 19-20: Malicious Email Spoofing Incidents
- Navigation and Vessel Inspection Circular (NVIC) 1-20: Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities.
- ISO 22301:2019: Security and resilience – Business continuity management systems – Requirements