News 09 Nov, 2020

USCG Issue Cyber Risk Management Guidelines

Cyber Risk Management Guidelines come into force on 1st January 2021 for all ships trading to the United States.

Key points:

- Every flag state is in scope
- Serious deficiencies will require fixing and an external audit within 90 days or risk detention
- Minor deficiencies will need an internal audit within 90 days and the deficiencies to be fixed prior to departure
- Inspections will only cover networked systems directly relevant to vessel safety
- Where faults have occurred in systems critical for vessel safety the inspector/port security control officer is mandated to investigate if the cause was 'cyber -related', and if so whether the right procedures were followed prior to that fault occurring
- If the inspector believes there are clear grounds for an expanded inspection, and clear evidence is gathered of poor implementation of the cyber risk management element of the SMS, further deficiencies may be issued
- The US Coast Guard document focuses on safety and security. Environmental protection remains in scope, but appears deemphasised in the USCG document

USCG Guidance to inspectors - Astaara view

Who does this affect?

All shipowners rigs and offshore units – of any flag state, that trade or operate in US.

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

What happens if my cyber security is found to be deficient?

Should there be any indications of compromise, inspectors are mandated to enquire further as to whether a deficiency exists, but only on systems required for the safe operation or navigation of the vessel. Standalone systems or other systems 'which do not affect the safe operation or navigation of the vessel" are not to be inspected or examined.

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.

What instructions do the inspectors have about deficiencies?

When deficiencies have been either revealed or identified, the inspector has three choices:

1. If cyber security risk management has not been incorporated into your SMS, the inspector can issue a deficiency with an action code 30 – ship detained.
2. If it is clear to the MI that while there is a cyber component to the ship's SMS, it is not being followed (as evidenced by poor cyber hygiene), The inspector can issue a deficiency in action code 17 – rectify prior to departure.
3. If or where there is evidence which suggests there has been a serious breach of cyber security in a vessel that has already incorporated cyber security into its SMS, the Marine inspector can issue a deficiency with the action code 30 – ship detained.

Can my ship be detained?

Yes. See above. In brief, if cyber risk management is not implemented or implemented in such a way that allows, or fails to prevent a cyber incident, the ship will either be subject to remediation of the deficiency before next US port visit “CODE 17- RECTIFY PRIOR TO DEPARTURE” or detained until remediation completed USCG will issue a A“CODE-30 SHIP DETAINED”.

If I have a deficiency what do I have to do?

Where there is a deficiency the owner will need to undertake an external audit within 3 months, and in any case, prior to re-entry into the US. If the deficiency is more about occasional lapses the owner will have to undertake an internal audit within 90 days. Or in the most serious cases prior to departure.

What if I am a US-flagged vessel?

Similar rules apply: If you are subject to the ISM Code as interpreted in CVC-WI-004(1) of 16 April 2018, you will be operating under regulations promulgated in 33 CFR Part 96 i.e. you will carry more than 12 passengers; displace more than 500GT; or be enrolled in the Alternative Compliance Programme. You will also be subject to CVC-WI-003 which details USCG Oversight of Safety Management Systems on US Flag Vessels.

Astaara Commentary

And so it begins. The US Coast Guard have fired the first salvo and have put operators of foreign flagged vessels on clear notice that if they arrive in a us port without the required (albeit very basic) cyber security / cyber hygiene, they risk being impounded, or at the very least being required to undertake rapid remediation.

There are indications in the document that cyber security will start to be regarded as a fundamental enabler for seaworthiness. It is also clear that the USCG is agnostic about which flag the vessel is travelling under – either they are compliant or they have deficiencies which need to be fixed – or the vessel will be seized. What is less clear is why USCG have in their guidance deliberately played down the requirement for cyber solutions to protect the environment.

What is helpful is the US Coast Guard has recognised that other frameworks for cyber risk assessment are in use (mention the work done by BIMCO for example and international organisations such as ISO/IEC). While they clearly prefer the NIST standard, they recognise that the IMO assessment follows the broad direction of this framework and therefore are prepared to work with it.

The USCG guidance is less helpful in that it only focuses on the ships only and fails to recognise the threat vector the head office represents. Nonetheless, it is clear what is expected – and clear about the consequences.

We have been warned.

Conclusion

This instruction has real teeth. Owners should ensure that every ship has clear documentation, standards and processes in place to ensure that Marine Inspector (“MI”)/Port State Control Officer (“PTSC”) has confidence in their approach to cybersecurity risk management. Even the smallest failure in a critical system requires urgent and professional remediation. If you arrive in the US port with a malfunctioning critical system, you will be required to fix it there and then, be audited, and be able to reassure the PSCO on your next visit that the issue has been rectified. If you cannot do this your vessel will be detained.