ABS REGULATORY NEWS
No. 04/2024

US COAST GUARD ENHANCING CYBERSECURITY

The growing utilization of networked technology in the maritime industry amplifies threats and vulnerabilities across telecommunications equipment, computers, and networks. To tackle this issue, the United States Coast Guard (USCG) authority has expanded to include cyber threats at sea. Vessels and offshore and port facilities will be required to strengthen their cyber defenses and comply with cybersecurity incident reporting rules.

KEY NOTES

Executive Order Empowers USCG to Enhance Cybersecurity Measures

References

- Part 6 of Title 33 of the Code of Federal Regulations
- Navigation and Vessel Inspection Circular 02-24
- Notice of Proposed Rulemaking: Cybersecurity in the Marine Transportation System

EXECUTIVE ORDER AUGMENTS USCG AUTHORITIES

On February 21, 2024, President Joe Biden signed an executive order which amended regulations regarding the safeguarding of vessels, harbors, ports and waterfront facilities of the United States (U.S.). The order specifically requires cyber threats to be considered through its updates to Part 6 of Title 33 of the Code of Federal Regulations (CFR).

Under the new regulations, the Captain of the Port (COTP) and the Commandant of the United States Coast Guard (USCG) are granted additional authorizations and powers to enhance cybersecurity measures.

Prevention of unauthorized access	The COTP has the authority to prevent the access of persons or things, including any data, information, network, program, system or other digital infrastructure to vessels or waterfront facilities. This measure aims to secure vessels and prevent damage or injury, including potential harm to digital infrastructure.
Establishment of security zones	Security zones can be established by the COTP, and entry into these zones without permission is prohibited. No person can board a vessel within a security zone or place any article or digital infrastructure on board without the COTP's authorization.
Inspection and search authority	The COTP, in accordance with the law, can conduct inspections and searches of vessels, waterfront facilities, security zones and persons. This includes examining any digital infrastructure, such as data, information, networks, programs, or systems, within the jurisdiction of the United States. The COTP can also place guards on vessels, waterfront facilities or security zones and remove unauthorized persons, articles or digital infrastructure.

Possession and control of vessels	The COTP has the power to supervise and control the movement of any vessel that presents a known or suspected cyber threat to U.S. maritime infrastructure. This authority allows the COTP to take full or partial possession or control of a vessel or its parts within U.S. territorial waters to secure it from damage or injury, including potential harm to digital infrastructure.
Safety measures	The Commandant is authorized to prescribe conditions and restrictions pertaining to the safety of waterfront facilities and vessels in port. Additionally, the Commandant has the authority to impose measures necessary to prevent, detect, assess, and remediate actual or threatened cyber incidents that could cause harm to vessels, harbors, ports, or waterfront facilities.

The executive order defines "cyber incident" and establishes a reporting requirement for these cyber incidents. Any evidence of sabotage, subversive activity, or an actual or threatened cyber incident endangering vessels, harbors, ports or waterfront facilities must be immediately reported to the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA) and the COTP.

The introduction of cyber incidents and the comprehensive scope of 33 CFR Part 6 led to an overlap with the existing reporting requirements outlined in the Maritime Transportation Security Act of 2002 (MTSA). To address this issue, the USCG issued Navigation and Vessel Inspection Circular (NVIC) 02-24, which offers clarification and voluntary guidance on reporting obligations specified in both 33 CFR Part 101 and 33 CFR Part 6.

USCG NVIC 02-24

NVIC 02-24 serves as a guidance document for complying with reporting requirements related to Breaches of Security (BOS), Suspicious Activity (SA), Transportation Security Incidents (TSI) and Cyber Incidents. NVIC 02-24 replaces the USCG's previous incident reporting guidance provided in CG-5P Policy Letter 08-16.

NVIC 02-24 specifies the following reporting procedures:

- Marine transportation system (MTS) stakeholders (i.e. any vessel, harbor, port or waterfront facility) are required to report acts of sabotage, subversive activity, or actual or threatened cyber incidents to the FBI, CISA and COTP, as per 33 CFR Part 6. They are also encouraged to report activities that could lead to a TSI to the National Response Center (NRC).
- MTSA-regulated entities (i.e. owners or operators of vessels, facilities or OCS facilities, regulated under MTSA in accordance with 33 CFR Parts 104, 105 or 106) must promptly report a BOS or SA to the NRC by dialing 1-800-424-8802, as per 33 CFR §101.305. Furthermore, owners or operators of vessels or facilities regulated under MTSA must immediately report a TSI to the local COTP and then follow the procedures outlined in their security plan, which may involve contacting the NRC. Owners or operators of OCS facilities regulated under MTSA must report a TSI to their respective District Commander without delay and then follow the procedures outlined in their security plan, which may involve contacting the NRC.

Enclosure (1) of NVIC 02-24 provides specific descriptions of incidents that fall within the categories of BOS, SA, or cyber incidents. It also includes descriptions of events that do not qualify as BOS, SA or cyber incidents.

Owners and operators are advised to consult these descriptions to determine if a situation meets the reporting criteria.

USCG NOTICE OF PROPOSED RULEMAKING

Given the expanded authority granted to the USCG, the USCG has published a Notice of Proposed Rulemaking (NPRM) through the Federal Register to update its maritime security regulations. The proposed update includes the addition of regulations specifically aimed at establishing minimum cybersecurity requirements for U.S.-flagged vessels, Outer Continental Shelf (OCS) facilities and U.S. facilities subject to the MTSA.

This proposed rule would introduce several requirements for owners or operators of U.S.-flagged vessels, facilities and OCS facilities. These requirements would include:

- Developing a Cybersecurity Plan that covers preparation, prevention and response to threats and vulnerabilities.
- Designating a Cybersecurity Officer (CySO).
- Conducting a Cybersecurity Assessment.
- Developing and submitting the Cybersecurity Plan to the USCG for approval.
- Operating U.S.-flagged vessels in accordance with the approved Cybersecurity Plan.
- Implementing security measures based on emerging cybersecurity vulnerabilities.
- Reporting any cyber incidents to the NRC.
- Performing cybersecurity drills and exercises in accordance with the Vessel Security Plan, Facility Security Plan and OCS Facility Security Plan.
- Maintaining records of cybersecurity-related information in either paper or electronic format.

Furthermore, the proposed rule would require the implementation of cybersecurity measures aimed at identifying risks, detecting threats and vulnerabilities, protecting critical systems and facilitating recovery from cyber incidents.

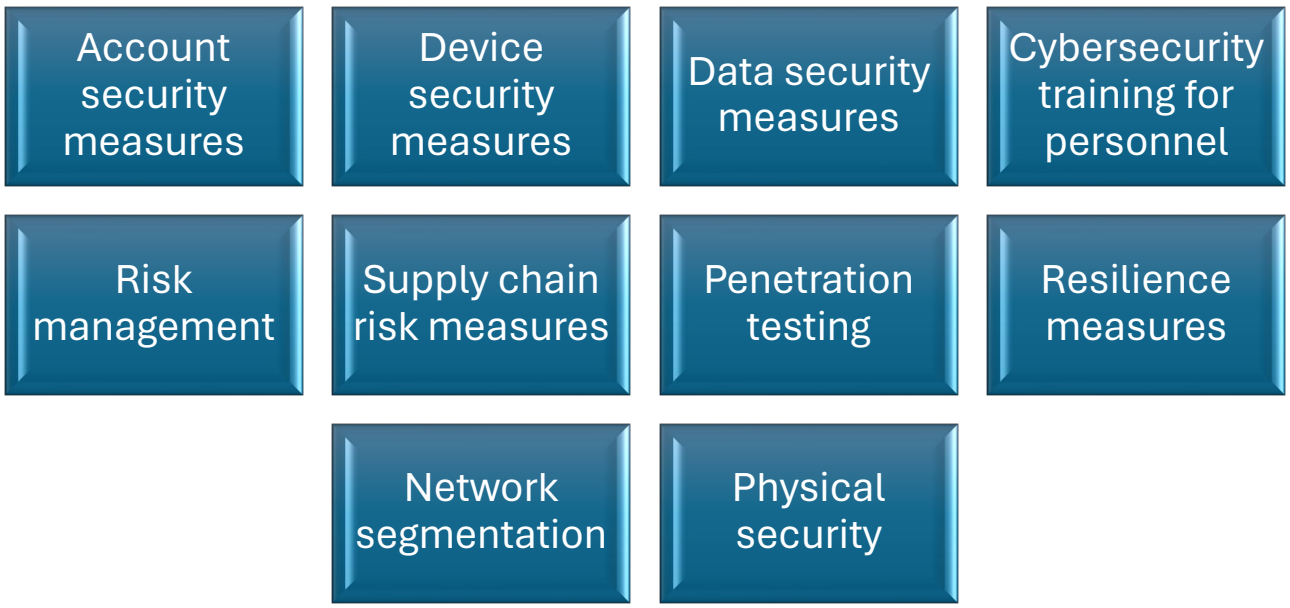

Figure 1: Cybersecurity measures according to the proposed rule.

Owners and operators would be granted flexibility by the USCG to determine the most suitable approach for implementing and adhering to these new requirements. The USCG proposes an implementation period of 12 to 18 months from the effective date of the final rule. This timeframe allows sufficient time for owners and operators of relevant U.S.-flagged vessels, U.S. facilities and OCS facilities to meet the requirements.

The USCG welcomes public participation in rulemaking and encourages comments and materials to be submitted by April 22, 2024, via www.regulations.gov.

IMO & IACS REQUIREMENTS

In 2017, the International Maritime Organization (IMO) addressed cybersecurity risks in the shipping industry by issuing the Marine Safety Committee/Facilitation Committee (MSC-FAL) Circular 3, *Guidelines on Maritime Cyber Risk Management* and MSC Resolution 428(98). The IMO emphasized that an approved Safety Management System (SMS) should incorporate Cyber Risk Management (CRM) to effectively address cybersecurity risks, aligning with the objectives and functional requirements of the International Safety Management (ISM) Code.

In April 2022, the International Association of Classification Societies (IACS) published the original versions of its Unified Requirements (UR) on cyber resilience:

- IACS UR E26 – Cyber Resilience of Ships.
- IACS UR E27 – Cyber Resilience of On-Board Systems and Equipment.

The IACS URs were formulated to establish a standardized set of minimum requirements, ensuring the delivery of vessels that meet the criteria of being cyber-resilient. Cyber-resilient vessels, systems and equipment include inherent safeguards against cyber incidents, and both the vessel and its crew are prepared with response measures in the event of such incidents.

In September 2023, IACS released the Rev. 1 version of UR E27, followed by the Rev. 1 version of UR E26 in November 2023. These revised versions superseded the original versions. Both URs are to be implemented by IACS Societies on ships contracted for construction on or after 1 July 2024, and may be used for other ships as non-mandatory guidance. For more information, please refer to *IACS Unified Requirements on Cyber Resilience* (ABS Regulatory News No. 14/2023).

WORLD HEADQUARTERS
1701 City Plaza Drive | Spring, TX 77389 USA
P 1-281-877-6000 | F 1-281-877-5976
ABS-WorldHQ@eagle.org
www.eagle.org