9110-04-P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG-2016-1084]

Navigation and Vessel Inspection Circular (NVIC) 05-17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities

AGENCY: Coast Guard, DHS

ACTION: Notice of availability and request for comments.

SUMMARY: The Coast Guard announces the availability of draft Navigation and Inspection Circular (NVIC) 05-17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities, and requests public comment on the draft. This NVIC proposes to clarify the existing requirements under MTSA to incorporate analysis of computer and cyber risks and guidance for addressing those risks. This NVIC would provide guidance on incorporating cybersecurity risks into an effective Facility Security Assessment (FSA), as well as additional recommendations for policies and procedures that may reduce cyber risk to operators of maritime facilities. Operators may use this document as a benchmark to develop and implement measures and activities for effective self-governance of cyber risks.

DATES: Comments must be submitted to the online docket via http://www.regulations.gov, or reach the Docket Management Facility, on or before [INSERT DATE [60] DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: If you have questions on this notice,

call or e-mail, Jason Warren, Coast Guard; telephone 202-372-1106, e-mail Jason.S.Warren@uscg.mil or LCDR Josephine Long, Coast Guard; telephone 202-372-1109, e-mail Josephine.A.Long@uscg.mil.

ADDRESSES: You may submit comments identified by docket number USCG-2016-1084 using the Federal eRulemaking Portal at http://www.regulations.gov. See the "Public Participation and Request for Comments" portion of the SUPPLEMENTARY INFORMATION section for further instructions on submitting comments.

SUPPLEMENTARY INFORMATION:

Public Participation and Request for Comments

We encourage you to submit comments (or related material) on the draft NVIC. We will consider all submissions and may adjust our final action based on your comments. If you submit a comment, please include the docket number for this notice, indicate the specific section of this document to which each comment applies, and provide a reason for each suggestion or recommendation.

We encourage you to submit comments through the Federal eRulemaking Portal at http://www.regulations.gov. If your material cannot be submitted using http://www.regulations.gov, contact the person in the FOR FURTHER INFORMATION CONTACT section of this document for alternate instructions. Documents mentioned in this notice, and all public comments, are in our online docket at http://www.regulations.gov and can be viewed by following that website's instructions. Additionally, if you go to the online docket and sign up for email alerts, you will be notified when comments are posted or a final rule is published.

We accept anonymous comments. All comments received will be posted without

change to http://www.regulations.gov and will include any personal information you have provided. For more about privacy and the docket, you may review a Privacy Act notice regarding the Federal Docket Management System in the March 24, 2005, issue of the Federal Register (70 FR 15086).

Discussion

As highlighted in the United States Coast Guard Cyber Strategy, cyber security is one of the most serious economic and national security challenges we face as a nation. Adversaries, including state-sponsored and independent hacker groups, terrorists, Transnational Organized Crime groups, and insider threats can pose significant threats to our nation's Marine Transportation System (MTS). Yet these same systems allow the MTS to operate with an impressive record of efficiency and reliability. With approximately 360 sea and river ports, which handle more than $1.3 trillion in annual cargo, we are dependent on a safe, secure, and efficient MTS, which in turn is highly dependent on a complex, globally-networked system of technology.

The maritime industry continues to increase use of cyber technology. Facility operators use computers and cyber dependent technologies for communications, engineering, cargo control, environmental control, access control, passenger and cargo screening, and many other purposes. Facility safety and security systems, such as security monitoring, fire detection, and general alarm installations increasingly rely on computers and networks. While these computer and network systems create benefits, they are inherently vulnerable and could introduce new vulnerabilities. Exploitation, misuse, or simple failure of cyber systems can cause injury or death, harm the marine environment, disrupt vital trade activity, and degrade the ability to respond to other

emergencies.

There are many resources, technical standards, and recommended practices available to the marine industry that can help their governance of cyber risks. Facility operators should use those resources to promote a culture of effective and proactive cyber risk management. The purpose of this draft NVIC is to begin to lay out a series of policies and procedures to mitigate these risks while ensuring the continued operational capability of the nation's MTS.

The provisions of the Maritime Transportation Security Act (MTSA) (Pub. L. 105-297, November 25, 2002) address the security of the MTS and authorize regulations. Under the authority of MTSA, the Coast Guard has promulgated regulations, located in subchapter H of Title 33 of the Code of Federal Regulations (CFR), which provide general parameters for port and facility security while allowing facility owners and operators the discretion to determine the details of how they will comply. Owners and operators are responsible for assessing vulnerabilities and ensuring the security of their facilities with Coast Guard oversight and guidance. The Coast Guard currently has the regulatory authority to instruct facilities and Outer Continental Shelf (OCS) facilities regulated under MTSA to address computer system and network vulnerabilities within their required Facility Security Assessment (FSA) and to address these vulnerabilities, if necessary, within the Facility Security Plan (FSP).

This draft NVIC would provide guidance and recommended practices for MTSA regulated facilities to address cyber-related vulnerabilities. It consists of two major parts. The first part, titled "Cyber Security and MTSA: 33 CFR parts 105 and 106," and labeled enclosure 1, discusses the existing MTSA regulatory requirements that are

applicable to cyber security related threats. These provisions , located in parts 105 and 106 of 33 CFR, currently require that owners and operators of MTSA-regulated facilities and OCS facilities conduct FSAs, and if applicable, include in their FSPs measures addressing any vulnerabilities identified in the FSA. The NVIC would lay out the Coast Guard's interpretation of these existing requirements as they would apply to cybersecurity threats and recommended additions to the FSP. As these regulations are currently in force, the recommendations of the NVIC, if finalized, would serve as the Coast Guard's interpretation of those regulations. The NVIC would assist the owner/operator in identifying cyber systems that are related to MTSA regulatory functions, or whose failure or exploitation could cause or contribute to a Transportation Security Incident.

This NVIC also contains a more detailed set of cybersecurity parameters, labeled as enclosure 2 and titled "Cyber Governance and Cyber Risk Management Program Implementation Guidance," which provides best recommended practices. This proposed guidance, derived from a variety of standardized industry practices including the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), lays out the basics for establishing a set of security policies designed to counter cybersecurity threats. These policies involve the establishment of roles and responsibilities for a Cyber Risk Management team, policies, and program, as well as guidance on how to implement such a program over a variety of business models. It also provides recommendations for developing security measures including inventory, access control, acceptable use policies, and network design. The recommendations in enclosure 2 of this proposed NVIC would provide the foundation for an effective strategy to help prevent and mitigate the damage

from cybersecurity threats to the MTS.

With the publication of this draft NVIC, the Coast Guard is seeking industry and public comments on the necessity, robustness, implementation, and costs of the proposed cybersecurity guidance. Specifically, we are seeking comments on the feasibility of its implementation, how flexible and useful it is in addressing the broad scope ofvulnerabilities and risk facing regulated facilities, and its ability to remain valid when technology and industry's use of technology changes. In addition, we seek comments on whether this guidance aligns with activities that may already be taking place by industry. The Coast Guard will carefully consider all comments submitted during the comment period before promulgating any final guidance. This notice is issued under authority of 5 U.S.C. 522(a).

R. D. Manning,
Captain, U.S. Coast Guard,
Chief, Office of Port and Facility Compliance
[FR Doc. 2017-14616 Filed: 7/11/2017 8:45 am; Publication Date: 7/12/2017]