9110-04-P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG-2014-1020]

Guidance on Maritime Cybersecurity Standards

AGENCY: Coast Guard, DHS.

ACTION: Notice with request for comments.

-

SUMMARY: The Coast Guard is developing policy to help vessel and facility operators identify and address cyber-related vulnerabilities that could contribute to a Transportation Security Incident. Coast Guard regulations require certain vessel and facility operators to conduct security assessments, and to develop security plans that address vulnerabilities identified by the security assessment. The Coast Guard is seeking public input from the maritime industry and other interested parties on how to identify and mitigate potential vulnerabilities to cyber-dependent systems. The Coast Guard will consider these public comments in developing relevant guidance, which may include standards, guidelines, and best practices to protect maritime critical infrastructure.

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].

ADDRESSES: Submit comments using one of the listed methods, and see

SUPPLEMENTAL INFORMATION for more information on public comments.

- Online – http://www.regulations.gov following website instructions.
- Fax – 202-493-2251.
- Mail or hand deliver – Docket Management Facility (M-30), U.S. Department of Transportation, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE., Washington, DC 20590-0001. Hours for hand delivery are 9 a.m. to 5 p.m., Monday through Friday, except Federal holidays (telephone 202-366-9329).

FOR FURTHER INFORMATION CONTACT: For information about this document call or e-mail LT Josephine Long, Coast Guard; telephone 202-372-1109, e-mail Josephine.A.Long@uscg.mil or LCDR Joshua Rose, Coast Guard; 202-372-1106, e-mail Joshua.D.Rose@uscg.mil. For information about viewing or submitting material to the docket, call Cheryl Collins, Program Manager, Docket Operations, telephone 202-366-9826, toll free 1-800-647-5527.

SUPPLEMENTARY INFORMATION:

Public Participation and Comments

We encourage you to submit comments (or related material) on the questions listed below. We will consider all submissions and may adjust our final policy actions based on your comments. Comments should be marked with docket number USCG-2014-1020, and should provide a reason for each suggestion or recommendation. You should provide personal contact information so that we can contact you if we have questions regarding your comments; but please note that all comments will be posted to the online docket without change and that any personal information you include can be

searchable online (see the Federal Register Privacy Act notice regarding our public dockets, 73 FR 3316, Jan. 17, 2008).

Mailed or hand-delivered comments should be in an unbound 8½ x 11 inch format suitable for reproduction. The Docket Management Facility will acknowledge receipt of mailed comments if you enclose a stamped, self-addressed postcard or envelope with your submission.

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 the website's instructions. You can also view the docket at the Docket Management Facility (see the mailing address under ADDRESSES) between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

Discussion

The Coast Guard is developing policy to help vessel and facility operators identify and address cyber-related vulnerabilities that could contribute to a Transportation Security Incident (TSI).[1] Coast Guard regulations require certain vessel and facility operators to conduct security assessments, and to develop security plans that address vulnerabilities identified by the security assessment.[2] Vessel and facility security plans must also address specific security functions, including the following:

- Communications
- Security Training Requirements
- Procedures for vessel/facility interfacing

[1] A Transportation Security Incident is defined in 33 CFR 101.105 to mean "a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area."

[2] 33 CFR parts 104 and 105, subparts C and D.

- Declaration of Security
- Security Systems and Equipment Maintenance
- Security Measures for Access Control
- Security Measures for Handling Cargo
- Security Measures for Monitoring
- Security Incident Procedures

The Coast Guard is seeking public input on the following questions:

(1) What cyber-dependent systems, commonly used in the maritime industry, could lead or contribute to a TSI if they failed, or were exploited by an adversary?

(2) What procedures or standards do vessel and facility operators now employ to identify potential cybersecurity vulnerabilities to their operations?

(3) Are there existing cybersecurity assurance programs in use by industry that the Coast Guard could recognize? If so, to what extent do these programs address vessel or facility systems that could lead to a TSI?

(4) To what extent do current security training programs for vessel and facility personnel address cybersecurity risks and best practices?

(5) What factors should determine when manual backups or other non-technical approaches are sufficient to address cybersecurity vulnerabilities?

(6) How can the Coast Guard leverage Alternative Security Programs[3] to help vessel and facility operators address cybersecurity risks?

[3] An Alternative Security Program is defined in 33 CFR 101.105 to mean "a third-party or industry organization developed standard that the Commandant [of the Coast Guard] has determined provides an equivalent level of security to that established by [33 CFR Chapter I, Subchapter H]."

(7) How can vessel and facility operators reliably demonstrate to the Coast Guard that critical cyber-systems meet appropriate technical or procedural standards?

(8) Do classification societies, protection and indemnity clubs, or insurers recognize cybersecurity best practices that could help the maritime industry and the Coast Guard address cybersecurity risks? (See also http://www.dhs.gov/publication/cybersecurity-insurance.)

Authority

This notice is issued under the authority of 5 U.S.C. 552(a).

Dated: December 12, 2014

Captain Andrew Tucci,
Chief, Office of Port & Facility Compliance,
U.S. Coast Guard

[FR Doc. 2014-29658 Filed 12/17/2014 at 8:45 am; Publication Date: 12/18/2014]