Inland Marine Expo 2019

Cyber Risk Management

LCDR Dan Mochen
Office of Port & Facility Compliance
Critical Infrastructure Protection Branch (CG-FAC-1)
U.S. Coast Guard Headquarters

Cyber Risk Management

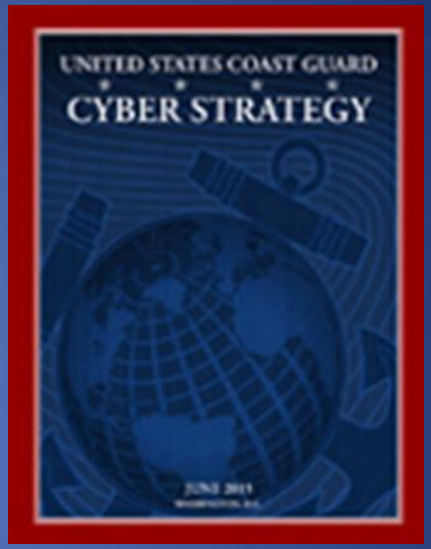
"Cyber threats collectively now exceed the danger of physical attacks against us. This is a major sea change for my department and for our country's security."

DHS Secretary Nielsen


The United States Coast Guard
CYBER RISK MANAGEMENT
LCDR DANIEL MOCHEN
LCDR BRANDON LINK
LT KELLEY EDWARDS
MR. CHARLES BLACKMORE
USCG

Cyber Risk Management

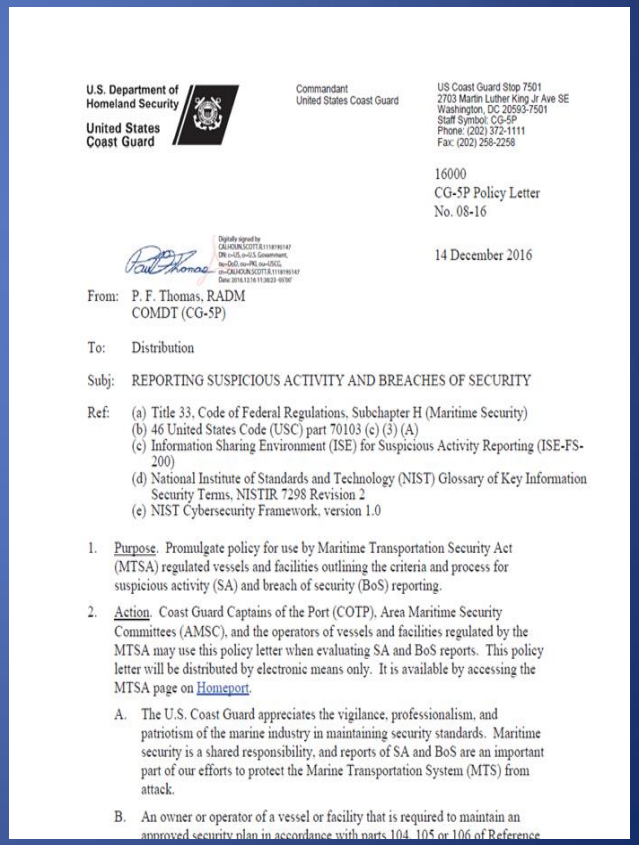
- Coast Guard Cyber Strategy
  - Three Strategic Priorities:
  1. Defending Cyberspace
  2. Enabling Operations
  3. Protecting Infrastructure



"We will ensure the security of our cyberspace, maintain superiority over our adversaries, and safeguard our Nation's critical maritime infrastructure"

Cyber Risk Management

- CG-5P Policy Letter 08-16
  - Reporting Suspicious Activity & Breaches of Security
    - Criteria for reporting Bos and/or SA for both physical & cyber related events
    - SA: Large, Sustained cyber attacks in an apparent attempt to exploit them
    - Reports to the NRC
    - National Cybersecurity & Communications Integration Center (NCCIC)
      - Cyber incidents only, do not involve physical or pollution effects



U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

US Coast Guard Stop 7501
2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7501
Staff Symbol: CG-5P
Phone: (202) 372-1111
Fax: (202) 258-2258

16000
CG-5P Policy Letter
No. 08-16

14 December 2016

From: P. F. Thomas, RADM
COMDT (CG-5P)

To: Distribution

Subj: REPORTING SUSPICIOUS ACTIVITY AND BREACHES OF SECURITY

Ref: (a) Title 33, Code of Federal Regulations, Subchapter H (Maritime Security)
(b) 46 United States Code (USC) part 70103 (c) (3) (A)
(c) Information Sharing Environment (ISE) for Suspicious Activity Reporting (ISE-FS-200)
(d) National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms, NISTIR 7298 Revision 2
(e) NIST Cybersecurity Framework, version 1.0

1. Purpose. Promulgate policy for use by Maritime Transportation Security Act (MTSA) regulated vessels and facilities outlining the criteria and process for suspicious activity (SA) and breach of security (BoS) reporting.

2. Action. Coast Guard Captains of the Port (COTP), Area Maritime Security Committees (AMSC), and the operators of vessels and facilities regulated by the MTSA may use this policy letter when evaluating SA and BoS reports. This policy letter will be distributed by electronic means only. It is available by accessing the MTSA page on Homeport.

A. The U.S. Coast Guard appreciates the vigilance, professionalism, and patriotism of the marine industry in maintaining security standards. Maritime security is a shared responsibility, and reports of SA and BoS are an important part of our efforts to protect the Marine Transportation System (MTS) from attack.

B. An owner or operator of a vessel or facility that is required to maintain an approved security plan in accordance with parts 104, 105 or 106 of Reference

Cyber Risk Management

- "Draft" Cyber NVIC – Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities
  - Guidance on incorporating computer systems & networks into FSAs & FSPs
  - Clarifies 33 CFR 105 & 106
  - 200+ comments on draft NVIC
  - Currently under review

COAST GUARD MARITIME COMMONS

THE COAST GUARD BLOG FOR MARITIME PROFESSIONALS

11/20/2017: Update on draft NVIC 05-17 – Guidelines for addressing cyber risks at MTSA facilities

Posted by LT Amy Midgett, Monday, November 20, 2017

Submitted by the Office of Port and Facility Compliance

The comment period for the draft Navigation and Vessel Inspection Circular (NVIC) 05-17 titled, "Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities" concluded Oct. 11, 2017, with more than 250 public comments submitted. The Coast Guard appreciates the feedback it received during the comment period.

Over the coming months, the Coast Guard will evaluate the comments and identify sections of NVIC 05-17 that would benefit from a more detailed explanation to improve clarity. Once the comments have been evaluated and NVIC 05-17 appropriately revised, the final document will be posted to the Federal Register.

The full list of public comments can be found on the Federal Register.

This blog is not a replacement or substitute for the formal posting of regulations and updates or existing processes for receiving formal feedback of the same. Links provided on this blog will direct the reader to official source documents, such as the Federal Register, Homeport and the Code of Federal Regulations. These documents remain the official source for regulatory information published by the Coast Guard.

Comments

comments

Tags: cyber risk, maritime transportation security act, navigation and vessel inspection circular

Search

About Us

Subscribe

RSS Feed

Submit Ideas

Categories

Bridge Programs
Commercial Vessel Compliance
– Domestic Vessels
– Fishing Vessels
– Foreign Vessels
Offshore
Congressional Hearings
Cyber Awareness & Risk Management
Design & Engineering Standards
– Lifesaving & Fire Safety
Emerging Policy
Environmental Response Policy
Federal Register
Investigations & Casualty Analysis
Mariner Credentialing
Navigation Systems
Operating & Environmental Standards
Ports and Facilities
– Cargo & Facilities

Cyber Risk Management

- Cybersecurity Framework Profiles
  - Customize the National Institute of Standards & Technology (NIST) Cybersecurity Framework.
  - Voluntary, non regulatory

What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

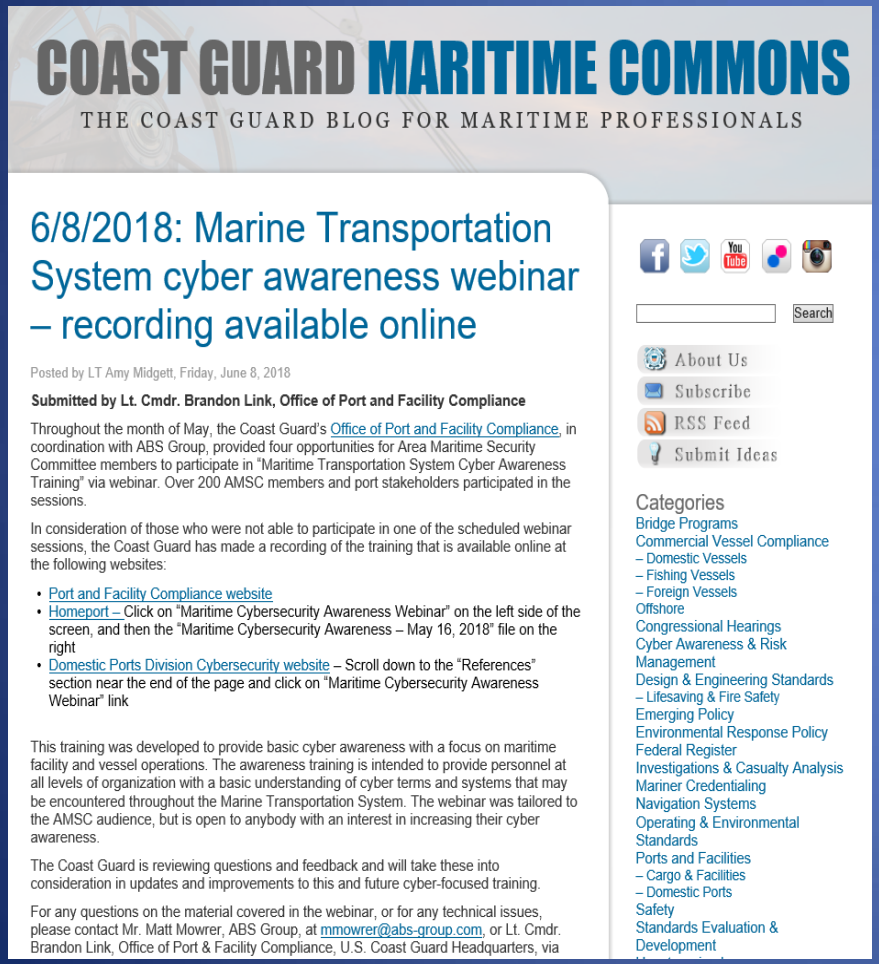
What techniques can contain impacts of incidents?

What techniques can restore capabilities?

Function	Category	Category Unique ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

Cyber Risk Management



COAST GUARD MARITIME COMMONS

THE COAST GUARD BLOG FOR MARITIME PROFESSIONALS

6/8/2018: Marine Transportation System cyber awareness webinar – recording available online

Posted by LT Amy Midgett, Friday, June 8, 2018

Submitted by Lt. Cmdr. Brandon Link, Office of Port and Facility Compliance

Throughout the month of May, the Coast Guard's Office of Port and Facility Compliance, in coordination with ABS Group, provided four opportunities for Area Maritime Security Committee members to participate in "Maritime Transportation System Cyber Awareness Training" via webinar. Over 200 AMSC members and port stakeholders participated in the sessions.

In consideration of those who were not able to participate in one of the scheduled webinar sessions, the Coast Guard has made a recording of the training that is available online at the following websites:

- Port and Facility Compliance website
- Homeport – Click on "Maritime Cybersecurity Awareness Webinar" on the left side of the screen, and then the "Maritime Cybersecurity Awareness – May 16, 2018" file on the right
- Domestic Ports Division Cybersecurity website – Scroll down to the "References" section near the end of the page and click on "Maritime Cybersecurity Awareness Webinar" link

This training was developed to provide basic cyber awareness with a focus on maritime facility and vessel operations. The awareness training is intended to provide personnel at all levels of organization with a basic understanding of cyber terms and systems that may be encountered throughout the Marine Transportation System. The webinar was tailored to the AMSC audience, but is open to anybody with an interest in increasing their cyber awareness.

The Coast Guard is reviewing questions and feedback and will take these into consideration in updates and improvements to this and future cyber-focused training.

For any questions on the material covered in the webinar, or for any technical issues, please contact Mr. Matt Mowrer, ABS Group, at mmowrer@abs-group.com, or Lt. Cmdr. Brandon Link, Office of Port & Facility Compliance, U.S. Coast Guard Headquarters, via

Search

About Us
Subscribe
RSS Feed
Submit Ideas

Categories

Bridge Programs
Commercial Vessel Compliance
– Domestic Vessels
– Fishing Vessels
– Foreign Vessels
Offshore
Congressional Hearings
Cyber Awareness & Risk Management
Design & Engineering Standards
– Lifesaving & Fire Safety
Emerging Policy
Environmental Response Policy
Federal Register
Investigations & Casualty Analysis
Mariner Credentialing
Navigation Systems
Operating & Environmental Standards
Ports and Facilities
– Cargo & Facilities
– Domestic Ports
Safety
Standards Evaluation & Development

Cyber Awareness Training

- 101 level awareness training
- Familiarity of cyber terms/issues in MTS
- Tailored to AMSC audience
- Available for all audiences

Cyber Risk Management

- FAA Reauthorization Act
  - "Develop & Implement a **Maritime Cybersecurity Risk Assessment Model** to evaluate current & future cybersecurity risk that have the potential to affect the MTS or would cause a TSI."
  - **Facility & Vessel Security Plans** to include detecting, responding to, and recovering from cybersecurity risks that may cause a TSI
- AMSC Cyber Subcommittee National Meetings

Cyber Risk Management

Commercial Vessels

Office of Design and Engineering (CG-ENG)

End Goal:
Implement a cyber risk management regime based on corporate governance and leveraging existing safety management systems.

Strategy:

Vessels	• IMO/SOLAS instruments and industry initiatives
Facilities	• MTSA authority and industry initiatives

Clear path to compliance:

MSC Resolution 428(98)

Maritime Cyber Risk Management in Safety Management Systems

Standards Development

- Appropriate standards will follow the Guidelines for Cyber Risk Management (MSC/FAL Circ. 3)

Incorporation of CRM into SMS

- Company selects an appropriate standard and incorporates those practices into their SMS

Review of SMS by RO

Recognized Organization (RO) reviews SMS during annual review

New DOC issued

New DOC is issued in accordance with MSC Resolution 428(98) prior to **1 January 2021**

Evaluation during SMS audits

SMS audits will provide feedback and verification

MTS Cyber Threats

THE COAST GUARD BLOG FOR MARITIME PROFESSIONALS

10/4/2018: National Cybersecurity Awareness Month: Cyber threats in the maritime environment

Posted by LT Amy Midgett, Thursday, October 4, 2018

October is National Cybersecurity Awareness Month and we'll be bringing you information throughout the month that focuses on cybersecurity, cyber risk management, and common practices you can employ now to safeguard your operations. This week, we have a post from our Domestic Ports Division on a few types of cyber threats your organization may encounter.

Written by Charles Blackmore, cyber program specialist, Office of Port & Facility Compliance

Monday, October 1 marked the start of National Cybersecurity Awareness Month. Our Nation's critical infrastructure and key resources are interlinked between physical and cyber security. This is especially true in the Marine Transportation System, as vessels and facilities increasingly rely on computer systems and networks to accomplish operations. Cyber threats require engagement from everyone – from local, state, and federal levels of government; private industry; and the public. Ensuring the cybersecurity of information systems, information technology, and operational technology requires constant vigilance and careful use both at an individual and organizational level.

Here are a few examples of cyber threats that can affect all industries and organizations, especially those in the maritime environment:

Phishing/Spear Phishing– Phishing is an attempt to induce individuals to reveal personal information such as passwords and credit card numbers. Spear phishing is a targeted attempt based on who the individual is (i.e. the company they work for). This is accomplished by trying to get an individual to download a file or click on a hyperlink. Users should be wary of emails received from people they do not know asking them to click on a link or download a file.

Search

About Us
Subscribe
RSS Feed
Submit Ideas

Categories
Bridge Programs
Commercial Vessel Compliance
– Domestic Vessels
– Fishing Vessels
– Foreign Vessels
Offshore
Congressional Hearings
Cyber Awareness & Risk Management
Design & Engineering Standards
– Lifesaving & Fire Safety
Emerging Policy
Environmental Response Policy
Federal Register
Investigations & Casualty Analysis
Mariner Credentialing
Navigation Systems
Operating & Environmental Standards
Ports and Facilities
– Cargo & Facilities

- Industrial Control Systems
  - Policies & Protocols
  - Built for Safety not Security
- 3rd Party Vendors
- Open/Default Passwords
- AIS & GPS Spoofing
- Spear Phishing
  - Malware
  - Ransomware
- Insider Threat

DHS NCATS

Service	Duration	Wait Time	Annual Capacity
Cyber Hygiene	Ongoing	None	No limit
Phishing Campaign Assessment	6 Weeks	~ 3 months	32
Validated Architecture Design Review	1 Week	~ 3 months	50
Risk & Vulnerability Assessment	2 Weeks	~ 9 months	60
Remote Penetration Test	4 Weeks	~ 6 months	64
Red Team Assessment	90 Days	~ 3 months	4

Email: ncats_info@hq.dhs.gov

Resources

COAST GUARD MARITIME COMMONS

THE COAST GUARD BLOG FOR MARITIME PROFESSIONALS

8/7/2017: Coast Guard seeking feedback on content of Passenger Operations Cybersecurity Framework Profile

Posted by LT Amy Midgett, Monday, August 7, 2017

The Office of Port and Facility Compliance (CG-FAC) announced today the release of a Content Preview of the Passenger Operations Cybersecurity Framework Profile, which is the result of a collaborative effort between the Coast Guard, the National Institute of Standards and Technology's (NIST) National Cybersecurity Center of Excellence, and key industry stakeholders in the field of safety and security.

The Content Preview highlights the approach to profile mission objectives in terms of cybersecurity, breaking them down into subcategories and assigning priority to each area related to cyber priorities.

A profile implements the NIST Cybersecurity Framework, which was developed in 2014 to address and manage cybersecurity risk in a cost-effective way based on business needs and without placing additional regulatory requirements on businesses. The profile is how organizations align the Framework's cybersecurity activities, outcomes, and informative references to organizational business requirements, risk tolerances, and resource allocations.

The first profile covering bulk liquid transfer operations was released Nov. 10, 2016.

CG-FAC invites the public to review the Content Preview and provide feedback. To comment, download and complete the comment matrix, and email it to HQS-SMB-CG-FAC-CYBER@uscg.mil by Sept. 7, 2017.

This blog is not a replacement or substitute for the formal posting of regulations and updates or existing processes for receiving formal feedback of the same. Links provided on this blog will direct the reader to official source documents, such as the Federal Register, Homeport and the Code of Federal Regulations. These documents remain the official source for regulatory information published by the Coast Guard.

Comments

comments

Tags: cybersecurity framework profile, national institute of standards and technology, passenger operations

Search

About Us
Subscribe
RSS Feed
Submit Ideas

Categories

Bridge Programs
Commercial Vessel Compliance
– Domestic Vessels
– Fishing Vessels
– Foreign Vessels
Offshore
Congressional Hearings
Cyber Awareness & Risk Management
Design & Engineering Standards
– Lifesaving & Fire Safety
Emerging Policy
Environmental Response Policy
Federal Register
Investigations & Casualty Analysis
Mariner Credentialing
Navigation Systems
Operating & Environmental Standards
Ports and Facilities
– Cargo & Facilities
– Domestic Ports
Safety
Standards Evaluation & Development
Uncategorized
Vessel Documentation
Waterways Policy

- CG Maritime Commons
- CG-FAC-1 Website
- ENG Website
- Homeport