NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
January 2023 (Edition 2023-01)

This **electronic** publication is intended to inform port stakeholders about cyber security issues and provide information useful to safeguard seaport systems that may be vulnerable to cyber-attacks. The information contained herein is suitable for general release and members of the Northern California Area Maritime Security Committee are encouraged to pass it on to members of our maritime community. This newsletter will be e-mailed to members of the Northern California Area Maritime Security Committee and posted on the Coast Guard's HOMEPORT portal within the Sector San Francisco port area.

IF YOU SEE SOMETHING, SAY SOMETHING

To report a crime in progress, call 911 or your local police department. To report maritime related suspicious activities or breaches of security call the National Response Center (NRC) at 800-424-8802 or if a **cyber-attack** to the National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870. After calling the NRC or NCCIC call the Captain of the Port, San Francisco, at 415-399-3530.

TABLE OF CONTENTS

ARTICLE SUMMARIES

- **Preparing for IMO's ISM Cyber Security –** a discussion about cyber risk management.
- **CISA Alerts** – a list of 2022 CISA alerts.
- **CISA Training Courses** – a list of current CISA training courses.

MAIN ARTICLES

Preparing for IMO's ISM Cyber Security, DNV, DNV.com, 30DEC2022

The ISM Code, supported by the IMO Resolution MSC.428(98), requires ship owners and managers to assess cyber risk and implement relevant measures across all functions of their safety management system, until the first Document of Compliance after 1 January 2021.

In combination with the resolution, the IMO also released Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) in July 2017. As both leave much of the interpretation to the company responsible for the safety management system, there are still many uncertainties of how to handle the requirements.
Below follow some concrete suggestions on how to ensure compliance with the IMO requirements and recommendations.

The IMO agreed that cyber risk management should be integrated into existing management systems under the ISM Code and ISPS Code. Accordingly, the following PDCA process should be applied:

Plan

The first step is to identify cyber security objectives relevant for the safe operation of the vessel. In addition to the IMO requirements, other internal and external stakeholder requirements on cyber security should be accounted for when determining the objectives. Pursuant to the defined objectives, an inventory list of all safety and business-critical systems and software should be generated. The inventory, as well as network drawings showing the system connectivity, are prerequisites for executing a cyber risk assessment. The assessment should include:

- Consequence analysis in terms of loss of confidentiality, integrity and availability of each system
- Likelihood analysis to determine how often the specific system is expected to be compromised
- Ranking of the asset according to its cyber security risks
- Determination of required barriers in terms of people, processes and technology improvements (for suggestions of barriers, see DNV's Cyber secure class notation)
  For more detailed information on how to execute cyber risk assessments for vessels and offshore assets, see our Recommended Practice **DNV-RP-0496** via the Rules and Standards Explorer.

Do

The cyber risk assessment results should be utilized to define an implementation plan for rolling out suitable barriers. Furthermore, as a minimum, the following functional requirements for the Safety Management System are applicable:

- A cyber security policy
- Instructions and procedures to ensure cyber-secure operation
- Defined levels of authority and lines of communication between, and amongst, shore and shipboard personnel concerning cyber security
- Procedures for reporting cyber-attacks, incidents and non-conformities
- Procedures to prepare for and respond to cyber-attacks and incidents
- Procedures for internal cyber security audits and management reviews
  DNV recommends executing different levels of training, including general awareness for all crew and personnel, as well as trainings for specific system users, on-board cyber security officers and internal auditors.

Check

The effectiveness of the cyber security measures must be checked on a continuous basis. Internal checks include:

- Evaluation of effectiveness of achieving cyber security objectives
- Analysis of cyber incident and event reports
- Evaluation of logs and intrusion detection systems
- Execution of internal audits of cyber security
- Execution of cyber security incident response drills

Furthermore, external checks are recommended in order to ensure:

- Increased cyber security resilience,
- Improved customer and business partner confidence, and
- Compliance with IMO requirements.

Act

Based on the findings of the internal and external review reports, corrective and preventive actions should be implemented. As the vessels and systems are increasingly interconnected and malicious cyber threats are continually changing, key to future successful cyber security resilience is to continuously improve by updating the cyber risk assessment, policies and procedures.

Preparing for IMO's ISM Cyber Security, By Paul Martin, USCG Sector San Francisco, 30DEC2022

The following is a list of 2022 Cyber and Infrastructure Security Agency (CISA) alerts:

- AA22-335A : #StopRansomware: Cuba Ransomware
- AA22-321A : #StopRansomware: Hive Ransomware
- AA22-320A : Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester
- AA22-294A : #StopRansomware: Daixin Team
- AA22-279A : Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors
- AA22-277A : Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization
- AA22-265A : Control System Defense: Know the Opponent
- AA22-264A : Iranian State Actors Conduct Cyber Operations Against the Government of Albania
- AA22-257A : Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations
- AA22-249A : #StopRansomware: Vice Society
- AA22-228A : Threat Actors Exploiting Multiple CVEs Against Zimbra Collaboration Suite
- AA22-223A : #StopRansomware: Zeppelin Ransomware

- AA22-216A : 2021 Top Malware Strains
- AA22-187A : North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector
- AA22-181A : #StopRansomware: MedusaLocker
- AA22-174A : Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems
- AA22-158A : People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices
- AA22-152A : Karakurt Data Extortion Group
- AA22-138B : Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control
- AA22-138A : Threat Actors Exploiting F5 BIG-IP CVE-2022-1388
- AA22-137A : Weak Security Controls and Practices Routinely Exploited for Initial Access
- AA22-131A : Protecting Against Cyber Threats to Managed Service Providers and their Customers
- AA22-117A : 2021 Top Routinely Exploited Vulnerabilities
- AA22-110A : Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
- AA22-108A : TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies
- AA22-103A : APT Cyber Tools Targeting ICS/SCADA Devices
- AA22-083A : Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector
- AA22-076A : Strengthening Cybersecurity of SATCOM Network Providers and Customers
- AA22-074A : Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability
- AA22-057A : Update: Destructive Malware Targeting Organizations in Ukraine
- A22-055A : Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks
- AA22-054A : New Sandworm Malware Cyclops Blink Replaces VPNFilter
- AA22-047A : Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology
- AA22-040A : 2021 Trends Show Increased Globalized Threat of Ransomware
- AA22-011A : Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

CISA Industrial Control System Advisories, CISA, CISA.gov, 30DEC2022

CISA released these Industrial Control Systems (ICS) advisories in December 2022. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.

CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations:

CSA-22-354-01 Fuji Electric Tellus Lite V-Simulator
ICSA-22-354-02 Rockwell Automation GuardLogix and ControlLogix

ICSA-22-354-03 ARC Informatique PcVue
ICSA-22-354-04 Rockwell Automation MicroLogix 1100 and 1400
ICSA-22-354-05 Delta 4G Router DX-3021
ICSA-22-349-01 Prosys OPC UA Simulation Server (Update A)
ICSA-22-356-01 Priva TopControl Suite
ICSA-22-356-02 Rockwell Automation Studio 5000 Logix Emulate
ICSA-22-356-03 Mitsubishi Electric MELSEC iQ-R, iQ-L Series and MELIPC Series
ICSA-22-356-04 Omron CX-Programmer

CISA Training Courses, CISA, CISA.gov, 30DEC2022

The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future. One way we accomplish this goal is by providing a robust offering of Cybersecurity and Critical Infrastructure Training opportunities.

Cybersecurity Training
Training is essential to preparing the cybersecurity workforce of tomorrow, and for keeping current cybersecurity workers up-to-date on skills and evolving threats. CISA is committed to providing the nation with access to cybersecurity training and workforce development efforts to develop a more resilient and capable cyber nation. Training areas include:

- NICCS Education and Training Catalog
- Formal Education
- Workforce Development
- On-Demand Cybersecurity Training
- Continuous Diagnostics and Mitigation (CDM) Training
- Industrial Control Systems
- Certification Offerings

Visit the Cybersecurity Training & Exercises page, as well as US-CERT's CDM Training and ICS Training pages for more information regarding these training opportunities.
Critical Infrastructure Training

CISA offers a wide array of free training programs to government and private sector partners. These web-based independent study courses, instructor-led courses, and associated training materials provide government officials and critical infrastructure owners and operators with the knowledge and skills needed to implement critical infrastructure security and resilience activities. Training areas include:

- Critical Infrastructure Independent Study Courses,
- Sector-Specific Training,
- Critical Infrastructure Security and Resilience Training Portal,
- Interagency Security Committee Training,
- Counter-Improvised Explosive Device (IED) Training and Awareness,
- Active Shooter Preparedness Workshops,

- Authorized User Training, and
- Other Training Resources.

Visit the Critical Infrastructure Training page for more information regarding these training opportunities.

Critical Infrastructure Learning Series

The Critical Infrastructure Learning Series provides one-hour, web-based seminars conducted by critical infrastructure experts on the tools, trends, issues, and best practices for infrastructure security and resilience.
Series offerings are available at no-cost and are highly recommended for the Department of Homeland Security's private sector and government partners, to include critical infrastructure owners and operators and officials with responsibility for risk, security, and emergency management functions.
Visit the Critical Infrastructure Learning Series page for more information regarding these webinars.

Insider Threat Training and Awareness

Videos and training courses are available to assist organizations prepare for and mitigate insider threats. Visit the Insider Threat Training and Awareness page for more information regarding these courses.

CVI Authorized User Training

CVI is used to protect information developed under the Chemical Facility Anti-Terrorism Standards (CFATS) regulation (6 CFR Part 27) that relates to vulnerabilities of high-risk chemical facilities that manufacture, use, store, or otherwise possess certain explosive, reactive, flammable, or toxic chemicals of interest, to terrorist attacks.
Only CVI Authorized Users with a need to know can have access to CVI.
Complete and submit the CVI training and the CVI Authorized User Application: Safeguarding Information Designated as Chemical-terrorism Vulnerability Information (CVI)
Note: This training does not make any determination on your need to know the CVI. The holder of the CVI or an appropriate Cybersecurity and Infrastructure Security Agency (CISA) official will make this decision each time a request for access to, or for disclosure of, CVI is made.
CISA will review the information you provide upon completion of this training and, if you are approved as a CVI Authorized User, CISA will notify you with an email providing a unique CVI Authorized User number and certificate to confirm your status.
Visit the CVI Authorized User Training page for more information.

Federal Virtual Training Environment (FedVTE)

The Federal Virtual Training Environment (FedVTE) is a free, online and on-demand cybersecurity training system. With courses ranging from beginner to advanced levels, you can strengthen or build your cybersecurity skillsets – at your own pace and schedule! FedVTE provides cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, U.S. military veterans and the public.

A limited number of courses are publicly available here:
https://fedvte.usalearning.gov/public_fedvte.php

Highlights include:

- Certification prep courses – Prepare and train for your next certification with our Certified Ethical Hacker, Cybersecurity Analyst (CySA+), Network +, Security +, Certified Information Security Manager (CISM), and Certified Information Systems Security Professional (CISSP) courses.
- Access – FedVTE courses can be completed at your own pace, at any time using your PC, laptop, or other mobile devices (i.e., smartphones, tablets).
- NICE Cybersecurity Workforce Framework – All courses are mapped to the NICE Framework Categories and Specialty Areas to help you identify courses that you need for your job or aspiration.

To register for an account or see the full course catalog, visit fedvte.usalearning.gov. For more information, visit niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte.
Visit the FedVTE page for more information about the courses being offered.

PCII Authorized User Training

To access Protected Critical Infrastructure Information (PCII), you must be a PCII Authorized User. However, access to individual items of PCII will be determined by your need to know that information. The holder of the PCII or an appropriate federal, state, tribal, or local government official will make this decision each time a request for access to or disclosure of PCII is made.
To apply for PCII Authorized User status, you must:

- Be a federal, state, tribal, or local government employee (or contractor);
- Complete training on the proper handling and safeguarding of PCII;
- Have homeland security responsibilities; and
- Sign a non-disclosure agreement (non-Federal employees only).

If you are unsure of your entity's status as belonging to either the public sector (e.g., a government entity) or private sector, please contact the Department of Homeland Security PCII Program at PCII-Assist@hq.dhs.gov.
Government contractors must also modify relevant contracts to comply with requirements of the PCII Program. Contract modification is not a prerequisite to accessing PCII; however, the contractor must contractually acknowledge his or her responsibilities with respect to PCII as

soon as practicable. The PCII Officer certifies that contractors are engaged in activities supporting their accredited entity.
Visit the PCII Authorized User Training page for more information.

Security and Awareness Training

Security and Awareness Training (SAT) Federal Shared Service Providers (FSSPs) provide common suites of information systems security training products and services for the federal government. SAT FSSPs provide standardized skills and competencies in order to align with nationally recognized credentials, such as the National Institute of Standards and Technology (NIST) guidance and the National Initiative for Cybersecurity Education (NICE), for government Information System Security (ISS) roles. The FSSPs provide a repository of government sponsored or approved training products and sources that will reach all levels of government executives.
Visit the Security and Awareness Training page for more information about the current offerings.

RBPS 11 Training

Risk-Based Performance Standard (RBPS) 11 – Training is the performance standard that addresses security and response training, exercises, and drills. By performing these properly, a facility prepares its personnel to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders.
A strong training program typically includes joint activities involving law enforcement and first responders to help them understand the layout and hazards involved with the facility.
Well-trained personnel who practice how to react will be more effective at detecting and delaying intruders as well as reducing the consequences of an attack.
Visit the RBPS 11 Training page for information available training and resources.

HOW YOU CAN HELP PROTECT CALIFORNIA

State, local, and tribal governments, non-governmental organizations and the private sector can partner with the Cal-CSIC by registering to receive Alerts and Advisories, sharing IOCs and cyber incident reports, and connecting to the California Automated Indicator Exchange.

- Email the Cal-CSIC to learn more about sharing of IOCs and connecting to the California Automated Indicator Exchange at calcsic@caloes.ca.gov.
- Report cyber incidents to the Cal-CSIC at (833) REPORT-1 or calcsic@caloes.ca.gov.

IMPORTANT NOTIFICATION CONTACT INFORMATION

Companies, facilities or vessels required to have a Marine Transportation Security Act (MTSA) security plan must report suspicious activities or breaches of security to the Coast Guard's National Response Center (NRC), or **cyber-attacks** to the National Cybersecurity and Communications Integration Center (NCCIC):

- (NRC) Phone 1-800-424-8802 or direct phone line at 202-372-2428

- (NRC) Fax 202-372-2920
- (NRC) Web: http://www.nrc.uscg.mil/
- (NCCIC) at 888-282-0870

After calling the NRC/NCCIC, call the Captain of the Port, San Francisco, at 415-399-3530.

Other agencies you may want to consider reporting to are:

California Cybersecurity Integration Center – (916) 636-2997 and CalCSIC@caloes.ca.gov

The Federal Bureau of Investigation (FBI) should be notified of cyber security breaches:

- FBI Headquarters – threats and crime reporting: https://tips.fbi.gov/
- San Francisco Office – 415-553-7400 (san.francisco@ic.fbi.gov)
- Sacramento Office – 916-841-9110 (http://www.fbi.gov/sacramento)
- Internet Crime Center – http://www.ic3.gov/complaint/default.aspx
- InfraGard Website – https://www.infragard.org/

U.S. COAST GUARD HOMEPORT PORTAL

The U.S. Coast Guard maintains links to various sources of maritime security information on its HOMEPORT information portal. The link to U.S. Coast Guard's HOMEPORT maritime security information portal is:

- Web – http://www.homeport.uscg.mil/

CUSTOMER FEEDBACK

How are we doing? Please send feedback about this newsletter to Mr. Paul Martin, USCG Sector San Francisco, at:

- E-mail – Paul.R.Martin@uscg.mil

Note: articles appearing in this newsletter were submitted by port stakeholders or downloaded from public websites and posted without editing. If you have an article to post, please provide the article to Mr. Martin at the above e-mail address. This newsletter is a quarterly publication and generally published shortly before a meeting of the Northern California Area Maritime Security Committee. **This newsletter is for public information purposes only**; articles containing proprietary, sensitive but unclassified, or classified information will not be accepted. The U.S. Coast Guard reserves the right to decide which articles are published in this newsletter.