# CYBERSECURITY FOR MARITIME FACILITIES

In support of the Maritime Subsector, the Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA), DHS/United States Coast Guard, DHS/Customs and Border Protection, Federal Bureau of Investigation (FBI), and Department of Transportation/Maritime Administration developed this infographic to introduce the use of the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity. This infographic also provides an overview of how and what to report to federal entities in the event of a significant cyber incident. This infographic is strictly informational and is intended for leadership within state, local, and private sector Maritime Subsector partners.

## IMPROVING MARITIME FACILITY CYBERSECURITY USING THE NIST FRAMEWORK

NIST's Framework for Improving Critical Infrastructure Cybersecurity, more commonly known as the Cybersecurity Framework, provides a flexible and common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices. The five Functions[1] of the NIST Cybersecurity Framework are:

### 1. IDENTIFY

Assists in developing an organizational understanding of cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related risks enables an organization to focus and prioritize its cybersecurity efforts, consistent with its risk management strategy and business needs.

### 2. PROTECT

Outlines appropriate safeguards to ensure delivery of critical infrastructure services, and supports the ability to limit or contain the impact of a potential cybersecurity event. This can include data protection, identity management, access control, and user awareness and training.

### 3. DETECT

Defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner.

### 4. RESPOND

Includes appropriate actions to take regarding a detected cybersecurity incident, and supports the ability to contain the impact of a potential cybersecurity incident.

### 5. RECOVER

Identifies appropriate measures to maintain resilience and restore any capabilities or services that were impaired due to a cybersecurity incident. Supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

To learn more about the NIST Cybersecurity Framework, visit **https://www.nist.gov/cyberframework**.

## REPORTING A CYBER INCIDENT

In the event of a cybersecurity incident resulting in significant impacts to information technology (IT) or operational technology (OT) systems, non-federal facilities in the Maritime Subsector should be ready to report an incident to appropriate authorities/organizations, including the U.S. Coast Guard, CISA's National Cybersecurity and Communications Integration Center (NCCIC), or the Federal Bureau of Investigation.

### U.S. Coast Guard

For MTSA[2]-regulated facilities or vessels, cybersecurity breaches or suspicious cyber activity should be reported to the Coast Guard's National Response Center (NRC). Guidelines for reporting a cyber-related incident can be found in CG-5P Policy Letter 08-16 titled "Reporting Suspicious Activity and Breaches of Security." The policy letter is available on the U.S. Coast Guard Homeport website[3] or contact your local Coast Guard Captain of the Port (COTP) for more details.

NRC contact information: 1-800-424-8802, **nrc@uscg.mil**

### CISA

CISA's NCCIC is a national nexus of cyber and communications integration for the Federal Government and may be able to provide technical assistance. MTSA-regulated facilities or vessels may report to CISA in lieu of the NRC if the cybersecurity incident involves no physical or pollution effects. The reporting party must inform CISA that they are a Coast Guard-regulated entity, and CISA's NCCIC will report the incident electronically to the NRC.

CISA's NCCIC contact information: 888-282-0870, **NCCICCustomerService@hq.dhs.gov**

### FBI

The FBI encourages victims to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch).

Field office contacts can be identified at **www.fbi.gov/contact-us/field**

CyWatch contact information: (855) 292-3937, **cywatch@fbi.gov**

FBI National Press Office contact information: (202) 324-3691, **npo@fbi.gov**

When reporting to U.S. Coast Guard, CISA, and FBI, non-technical information provides critical context facilitating appropriate assistance. Non-technical information includes incident location, physical address, type of facility, a brief summary of activity, and the impact to the facility.

While not a requirement, CISA and FBI can use technical data provided by the victim in order to assist in mitigating and investigating the incident. Technical information of potential use includes log files, source ports involved in the attack, indications of sophisticated tactics, techniques, and procedures (TTPs), indications that the attack specifically targeted the victim, status change data, and time stamps.

[1]NIST. The Five Functions. Last modified August 10, 2018. **www.nist.gov/cyberframework/online-learning/five-functions**. Accessed April 2, 2019.
[2]MTSA. Maritime Transportation Security Act of 2002.
[3]U.S. Coast Guard. CG-5P Policy Letter No. 08-16: Reporting Suspicious Activity and Breaches of Security. **https://homeport.uscg.mil/Lists/Content/Attachments/2676/CG-5P%20Policy%20Letter%2008-16_3.pdf**. Accessed April 2, 2019.