NATIONAL RISK MANAGEMENT CENTER

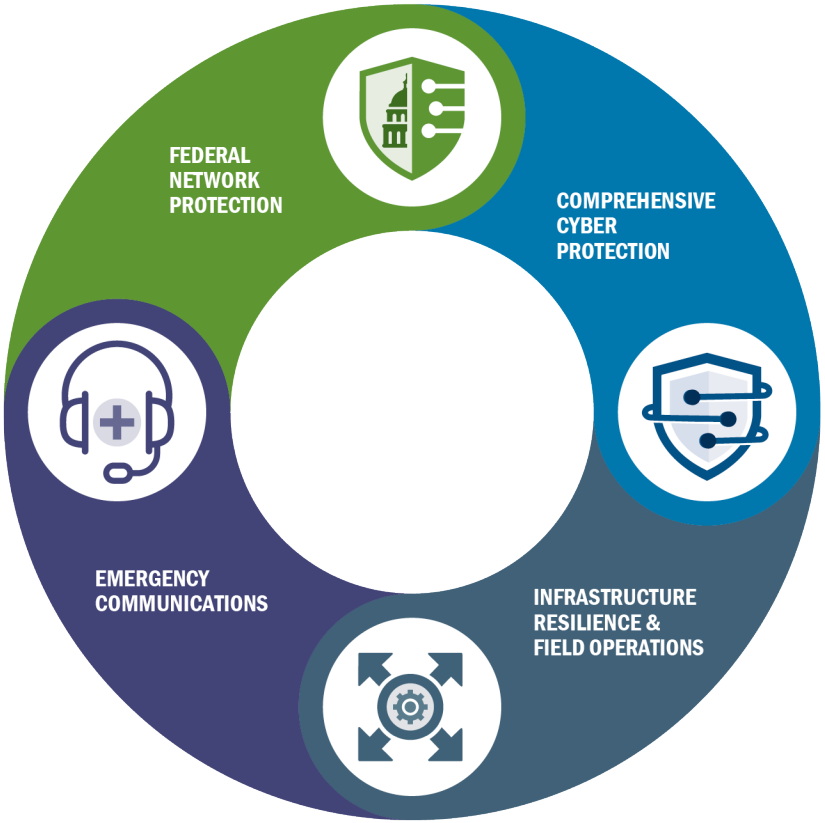
PRESENTATION FOR THE MARITIME RISK SYMPOSIUM 2019

FUTURE RISK PANEL DISCUSSION

CISA
CYBER+INFRASTRUCTURE

We are the Nation's Risk Advisors

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure



CISA
CYBER+INFRASTRUCTURE

NRMC – Planning and Analysis

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

National Risk Management Center

The NRMC is a planning, analysis, and collaboration center. CISA coordinates with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage risks to National Critical Functions, which are vital to the United States.

MISSION PRIORITIES:

- Analyzes most strategic risks to our Nation's Critical Infrastructure
- Leads public/private partnership initiatives to manage priority area of national risk
- Collaborates with private sector and other stakeholders to better understand future threats

Emerging Risk Landscape

1. **Nation states and criminal actors continue to target American critical infrastructure.**
   - NotPetya (2017): Russian destructive malware attack resulting in over $10 billion in damages globally, including hundreds of millions in damages to Maritime Subsector.
2. **Cross-sector reality.** Critical infrastructure risk management, particularly around cybersecurity, is increasingly cross-sector in nature.
3. **Our understanding of risk must evolve** from a static asset/organization view to a more holistic approach that focuses on functions and services.

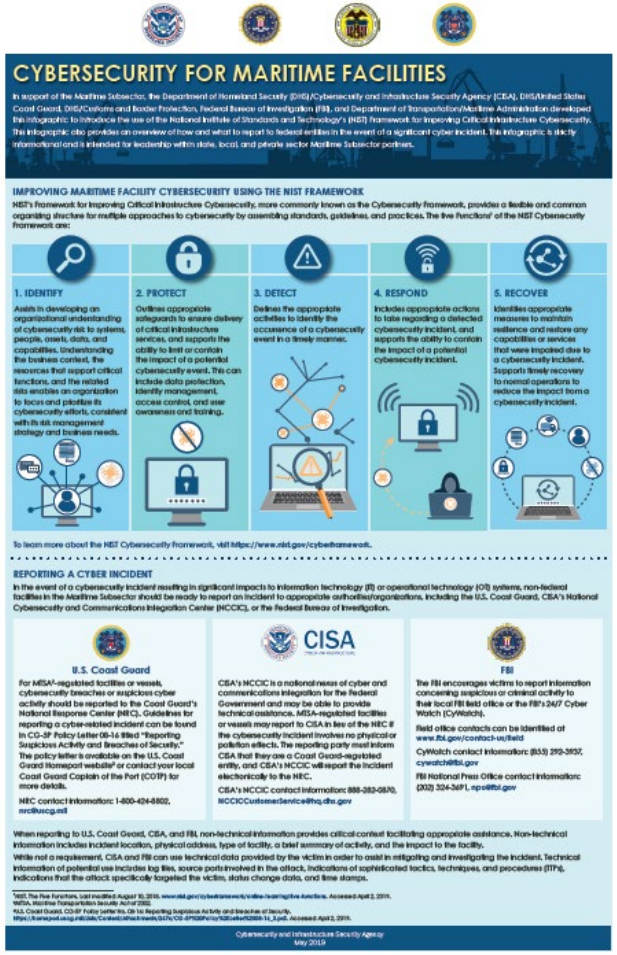
National Critical Functions Set

CONNECT	DISTRIBUTE	MANAGE	SUPPLY
▪ Operate Core Network ▪ Provide Cable Access Network Services ▪ Provide Internet Based Content, Information, and Communication Services ▪ Provide Internet Routing, Access and Connection Services ▪ Provide Positioning, Navigation, and Timing Services ▪ Provide Radio Broadcast Access Network Services ▪ Provide Satellite Access Network Services ▪ Provide Wireless Access Network Services ▪ Provide Wireline Access Network Services	▪ Distribute Electricity ▪ Maintain Supply Chains ▪ Transmit Electricity ▪ Transport Cargo and Passengers by Air ▪ Transport Cargo and Passengers by Rail ▪ Transport Cargo and Passengers by Road ▪ Transport Cargo and Passengers by Vessel ▪ Transport Materials by Pipeline ▪ Transport Passengers by Mass Transit	▪ Conduct Elections ▪ Develop and Maintain Public Works and Services ▪ Educate and Train ▪ Enforce Law ▪ Maintain Access to Medical Records ▪ Manage Hazardous Materials ▪ Manage Wastewater ▪ Operate Government ▪ Perform Cyber Incident Management Capabilities ▪ Prepare For and Manage Emergencies ▪ Preserve Constitutional Rights ▪ Protect Sensitive Information ▪ Provide and Maintain Infrastructure ▪ Provide Capital Markets and Investment Activities ▪ Provide Consumer and Commercial Banking Services ▪ Provide Funding and Liquidity Services ▪ Provide Identity Management and Associated Trust Support Services ▪ Provide Insurance Services ▪ Provide Medical Care ▪ Provide Payment, Clearing, and Settlement Services ▪ Provide Public Safety ▪ Provide Wholesale Funding ▪ Store Fuel and Maintain Reserves ▪ Support Community Health	▪ Exploration and Extraction Of Fuels ▪ Fuel Refining and Processing Fuels ▪ Generate Electricity ▪ Manufacture Equipment ▪ Produce and Provide Agricultural Products and Services ▪ Produce and Provide Human and Animal Food Products and Services ▪ Produce Chemicals ▪ Provide Metals and Materials ▪ Provide Housing ▪ Provide Information Technology Products and Services ▪ Provide Materiel and Operational Support to Defense ▪ Research and Development ▪ Supply Water

Cybersecurity Risk To Maritime Subsector

1. **Most organizations in the Maritime Subsector are aware of the cybersecurity risks to their operations, but these risks continue to grow**
   - Continued increase in terminal throughput that requires advanced systems and technology to operate
   - Vessel and terminal equipment automation will continue to spread as technologies become more affordable and reliable
   - Increased reliance on technology by new mariners/landside personnel
2. **The capabilities of both criminals and nation states will also increase, as will the effects than can be caused by their malicious cyber activities**

Cybersecurity for Maritime Facilities Infographic



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 solely 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 MISA[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. MISA-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, 2016, 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/cgib/Content/attachments/DJ76/CG-5PSOP/Policy%20Letter%2008-16_1.pdf. Accessed April 2, 2019.

Cybersecurity and Infrastructure Security Agency
May 2019

- Joint product between CISA, USCG, CBP, FBI, and DOT
- Highlights five functions of the NIST Cybersecurity Framework
- Details how to report a cybersecurity incident to USCG, CISA, and FBI, and what details to provide

CISA CYBER+INFRASTRUCTURE

NRMC Initiatives and Future Maritime Risks

NRMC is leading multiple initiatives in areas that impact future maritime risks

- Information and Communications Technology (ICT) Supply Chain
  - What are the connected devices in the maritime domain that need high levels of trust and assurance? How is that trust achieved?
- Fifth Generation Cellular Networks (5G)
  - How can maritime transportations use 5G-enabled technologies and still limit consequences from disruption, dysfunction or corruption?
- Position, Navigation and Timing (PNT)
  - How can maritime industries continue to utilize PNT technologies while minimizing impacts from potential disruptions?

NCF Failures beyond Disruption

"National Critical Functions" means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

- CISA built on the definition of critical infrastructure, but expanded to address corruption and dysfunction.
  - How can maritime systems be planned and engineered to address failures from corruption or dysfunction, as might result from a cyber attack?

CISA

CYBER+INFRASTRUCTURE