DigiMariner
MaritimeTV Event

CAPT Glenn Hernandez, USCG (Ret)
USCGA Class of 1991

November 18, 2020

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

- NIST NICE Main Site
- Employer Resources
- FREE or Low Cost On-line Learning Content

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

- https://www.cyberseek.org/

NICE Working Group

- Full Working Group: 4 Monthly Meetings (January, February, March, April)

Subgroups

- Apprenticeship Subgroup
- Collegiate Subgroup
- Competitions Subgroup
- K12 Subgroup
- Training and Certifications Subgroup
- Workforce Management Subgroup

NICE Interagency Coordinating Council

- Meetings: 4 Monthly Meetings (January, February, March, April)
- For additional information please visit here.

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

- NICCS Main Site
- Workforce Framework
- Workforce Mapping Tool
- Cyber Career Pathways

CYBERSPACE SOLARIUM COMMISSION

Introduction

- The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The finished report was presented to the public on March 11, 2020.

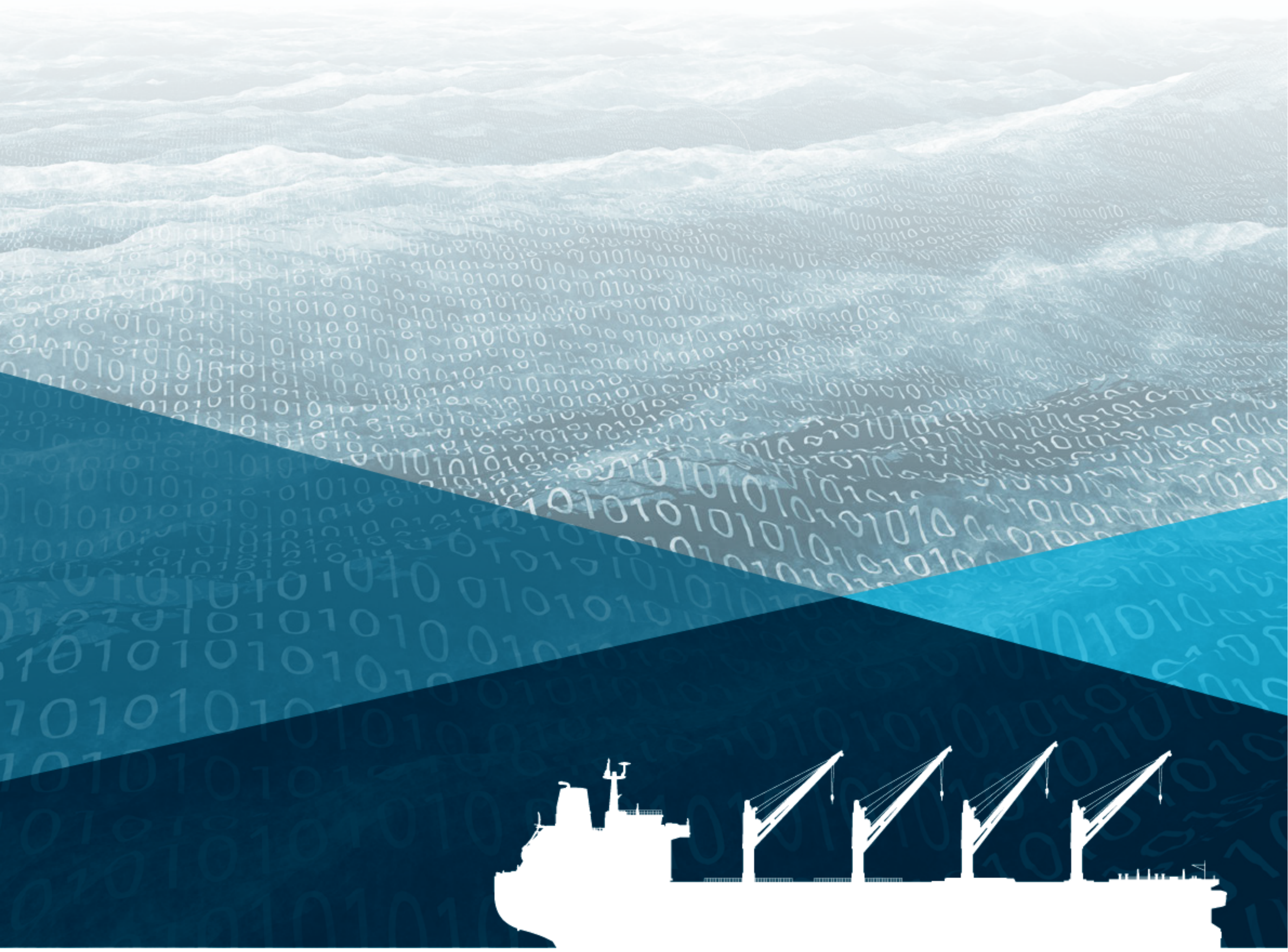
The Commission Report

- The Cyberspace Solarium Commission's proposes a strategy of layered cyber deterrence. Our report consists of over 80 recommendations to implement the strategy. These recommendations are organized into 6 pillars:
  - ***Reform the U.S. Government's Structure and Organization for Cyberspace.***
  - ***Strengthen Norms and Non-Military Tools.***
  - ***Promote National Resilience.***
  - ***Reshape the Cyber Ecosystem.***
  - ***Operationalize Cybersecurity Collaboration with the Private Sector.***
  - ***Preserve and Employ the Military Instrument of National Power.***

GROWING A STRONGER FEDERAL CYBER WORKFORCE

On September 4, 2020, the Cyberspace Solarium Commission released, "Growing a Stronger Federal Cyber Workforce." This paper reemphasizes the Commission's prior recommendations on the cyber workforce and presents a detailed blueprint to guide the development of a comprehensive Federal cyber workforce strategy.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS



Produced and supported by

BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL

v3

IMO INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3
5 July 2017

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

***

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

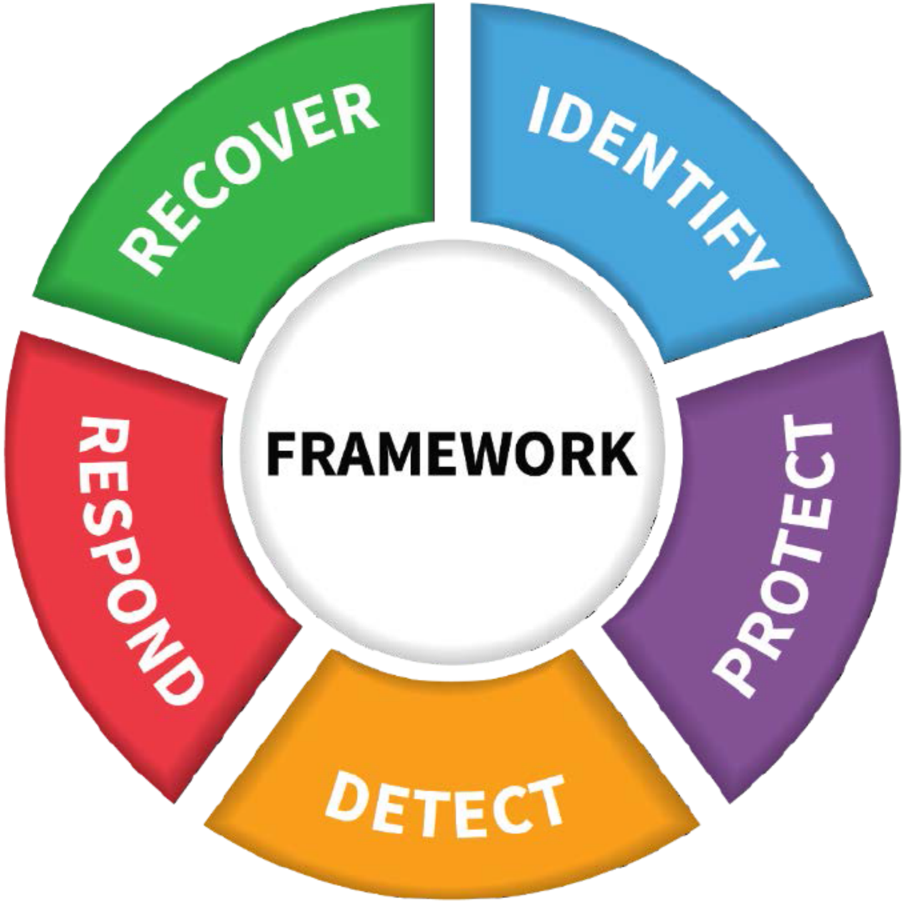
2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

***

Cybersecurity Framework Functions



Credit: N. Hanacek/NIST

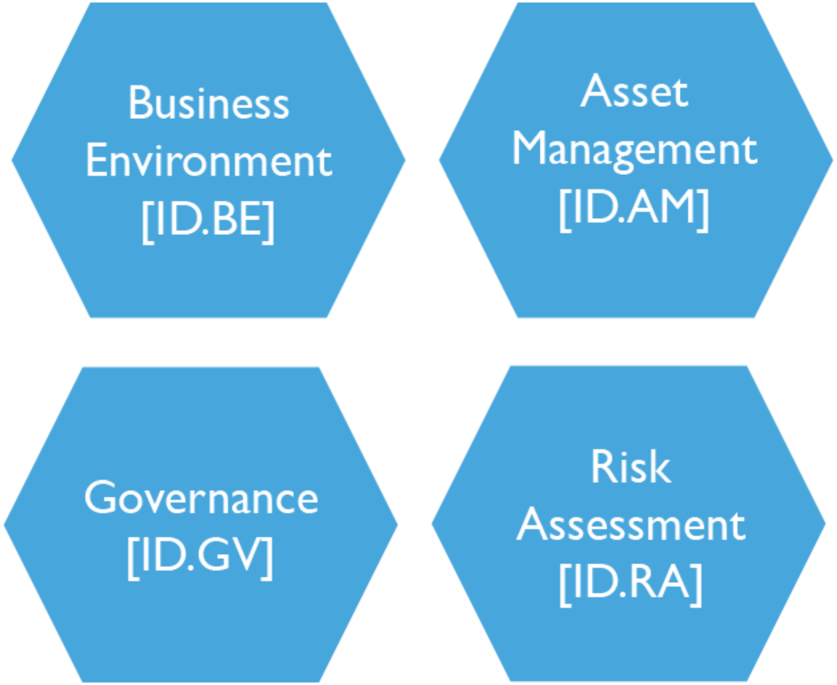
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
FRAMEWORK

Identify

Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Sample Identify Activities

FRAMEWORK
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER



Business Environment [ID.BE]

Asset Management [ID.AM]

Governance [ID.GV]

Risk Assessment [ID.RA]

- Identify critical business processes
- Document Information flows
- Establish policies for cybersecurity that includes roles and responsibilities
- Maintain hardware and software inventory
- Identify contracts with external partners
- Identify Risk Management processes

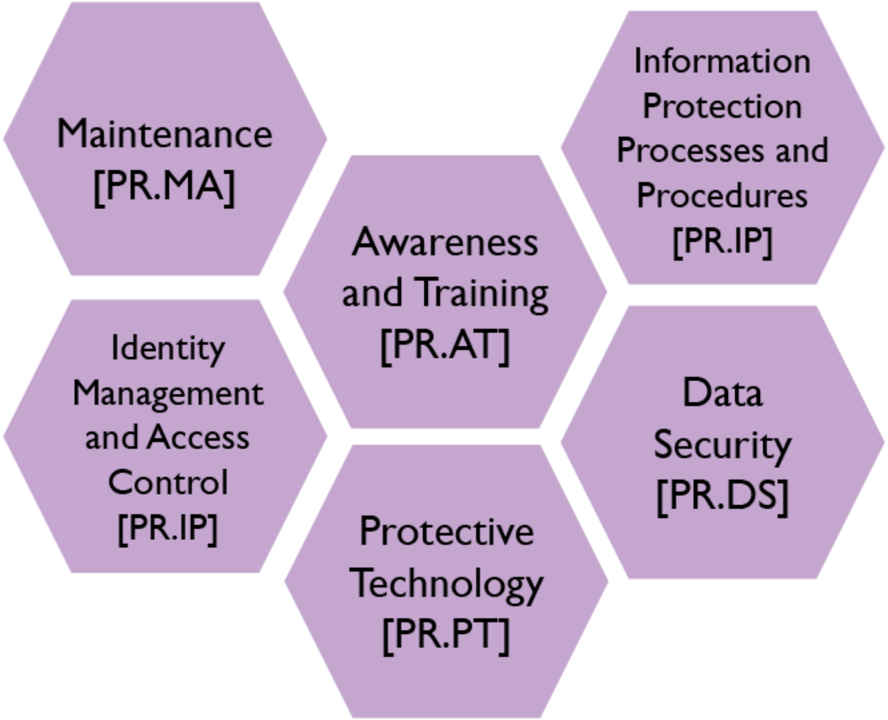
RECOVER
IDENTIFY
FRAMEWORK
RESPOND
PROTECT
DETECT

Protect

Develop and implement the appropriate safeguards to ensure delivery of services.

Sample Protect Activities

RECOVER
IDENTIFY
FRAMEWORK
PROTECT
RESPOND
DETECT



Maintenance [PR.MA]

Awareness and Training [PR.AT]

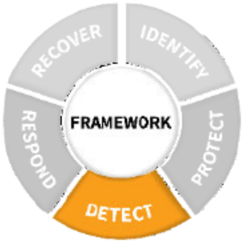
Information Protection Processes and Procedures [PR.IP]

Identity Management and Access Control [PR.IP]

Data Security [PR.DS]

Protective Technology [PR.PT]

- Manage access to assets and information
- Conduct regular backups
- Protect sensitive data
- Patch operating systems and applications
- Create response and recovery plans
- Protect your network
- Train your employees



Detect

Develop and implement the appropriate activities to **identify the occurrence of a cybersecurity event.**

Sample Detect Activities

Anomalies and Events [DE.AE]

Continuous Monitoring [DE.CM]

- Install and update anti-virus and other malware detection software
- Know what are expected data flows for your business
- Maintain and monitor logs

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
FRAMEWORK

Respond

Develop and implement the appropriate activities to **take action regarding a detected cybersecurity event.**

Sample Respond Activities

Response Planning [RS.RP]

Communications [RS.CO]

- Coordinate with internal and external stakeholders
- Ensure response plans are tested
- Ensure response plans are updated

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
FRAMEWORK

Recover

Develop and implement the appropriate activities to maintain plans for **resilience and to restore any capabilities or services** that were impaired due to a cybersecurity event.

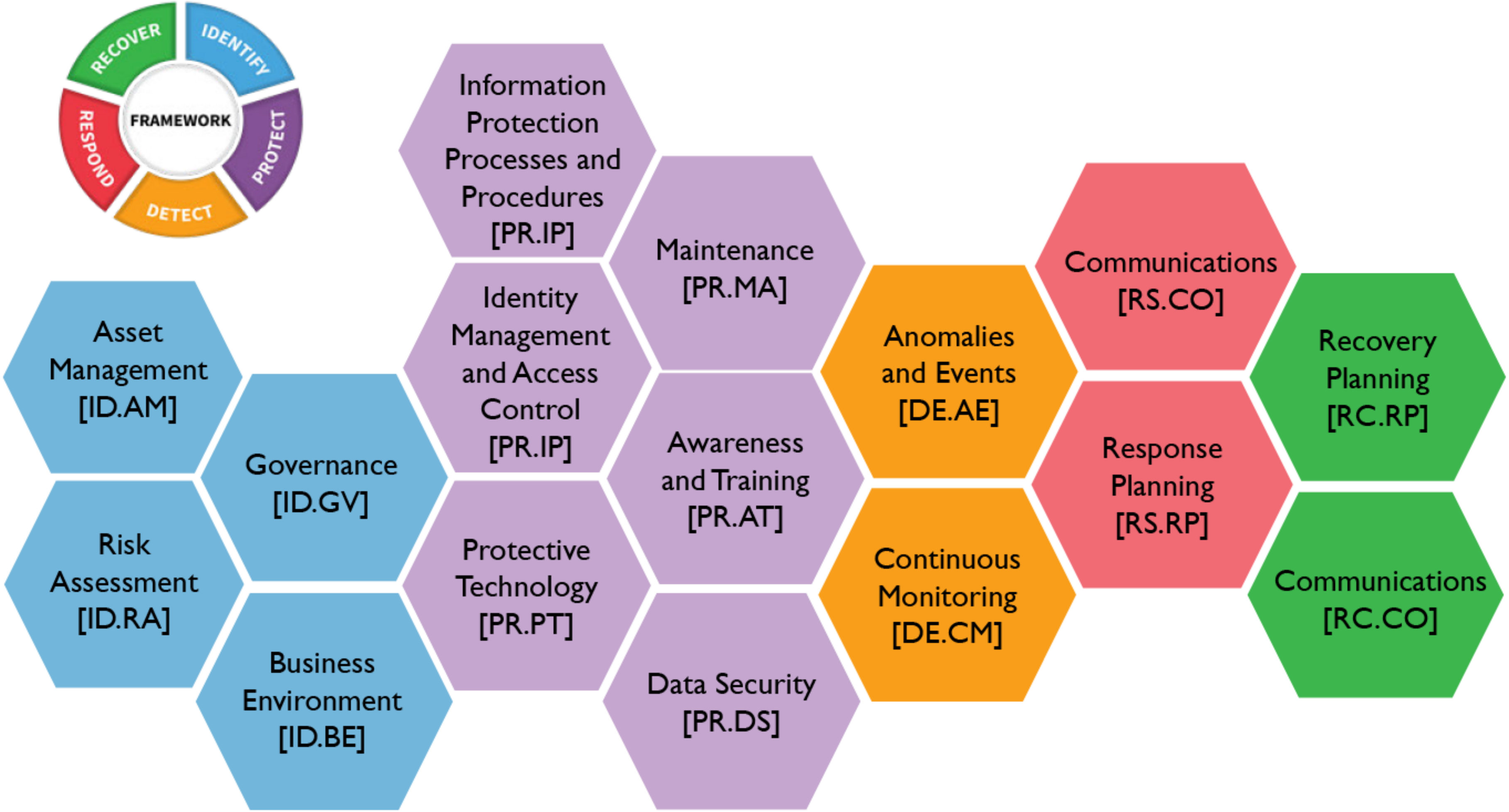
Sample Recover Activities

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
FRAMEWORK

Recovery Planning [RC.RP]

Communications [RC.CO]

- Manage public relations and company reputation
- Communicate with internal and external stakeholders
- Ensure recovery plans are updated
- Consider cyber insurance



Asset Management [ID.AM]

Risk Assessment [ID.RA]

Governance [ID.GV]

Business Environment [ID.BE]

Information Protection Processes and Procedures [PR.IP]

Identity Management and Access Control [PR.IP]

Protective Technology [PR.PT]

Maintenance [PR.MA]

Awareness and Training [PR.AT]

Data Security [PR.DS]

Anomalies and Events [DE.AE]

Continuous Monitoring [DE.CM]

Communications [RS.CO]

Response Planning [RS.RP]

Recovery Planning [RC.RP]

Communications [RC.CO]

UNITED STATES COAST GUARD

CYBER STRATEGY

JUNE 2015

WASHINGTON, D.C.

U.S. Department of Homeland Security

United States Coast Guard

Commandant
U.S. Coast Guard

2703 Martin Luther King Jr. Ave
Washington, DC 20593-7618
Staff Symbol: CG-FAC
Phone: (202) 372-1107

COMDTPUB P16700.4
NVIC 01-20
February 26, 2020

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 01-20

Subj: GUIDELINES FOR ADDRESSING CYBER RISKS AT MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATED FACILITIES

Ref: (a) Title 33 of the Code of Federal Regulations (CFR) Subchapter H, Maritime Security

1. PURPOSE. This Navigation and Vessel Inspection Circular (NVIC) provides guidance to facility owners and operators in complying with the requirements to assess, document, and address computer system or network vulnerabilities. In accordance with 33 CFR parts 105 and 106, which implement the Maritime Transportation Security Act (MTSA) of 2002 as codified in 46 U.S.C. Chapter 701, regulated facilities (including Outer Continental Shelf facilities) are required to assess and document vulnerabilities associated with their computer systems and networks in a Facility Security Assessment (FSA). If vulnerabilities are identified, the applicable sections of the Facility Security Plan (FSP) must address the vulnerabilities in accordance with 33 CFR 105.400 and 106.400.

2. DISCLAIMER. This NVIC is intended only to provide clarity regarding existing requirements under the law. It does not change any legal requirements, and does not impose new requirements on the public. Not all recommendations will apply to all facilities, depending on individual facility operations. Facility owners and operators may use a different approach that has greater or lesser complexity than this NVIC recommends, if that approach satisfies the applicable legal requirements (*i.e.*, this NVIC does not represent a minimum requirement for compliance).

3. ACTION.

a. Enclosure (1) provides a list of existing MTSA regulatory requirements that may apply once a facility owner or operator identifies computer system and/or network vulnerabilities in

DISTRIBUTION - SDL No. 170

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B	X	X	X		X									X										X		
C					X																				X	
D				X							X															
E					X									X				X								
F																										
G																										
H						X				X																

NON-STANDARD DISTRIBUTION

USCG Office of Commercial Vessel Compliance (CG-CVC)
Mission Management System (MMS) Work Instruction (WI)

Category	Commercial Vessel Compliance (Domestic and Foreign Vessels)				
Title	Vessel Cyber Risk Management Work Instruction				
Serial	CVC-WI-027(1)	Orig. Date	27OCT20	Rev. Date	N/A
Disclaimer:	This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is not intended to nor does it impose legally binding requirements on any part. It represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the public, and the Coast Guard, as well as other federal and state regulators, in applying statutory and regulatory requirements. You can use an alternative approach for complying with these requirements if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative approach (you are not required to do so), you may contact the Coast Guard Office of Commercial Vessel Compliance (CG-CVC) at CG-CVC@uscg.mil who is responsible for implementing this guidance.				
References:	(a) Maritime Safety Committee Resolution 428(98), "Maritime Cyber Risk Management in Safety Management Systems" (b) U.S. Coast Guard Cyber Strategy, June 2015 (c) International Safety Management (ISM) Code (d) U.S. Flag Interpretations on the ISM Code, (CVC-WI-004(1)) (e) Title 33 Code of Federal Regulations (CFR) Part 96 (f) Chapter IX, Management of the Safe Operation of Ships, International Convention for the Safety of Life at Sea (SOLAS), 1974 (g) Title 33 Code of Federal Regulations (CFR) Subchapter H (h) National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, April 16, 2018 (i) Navigation and Vessel Inspection Circular (NVIC) 04-05: "Port State Control Guidelines for the Enforcement of Management for the Safe Operation of Ships (ISM Code)" (j) "Guidelines for Port State Control Officers on the International Safety Management (ISM) Code," MSC-MEPC.4/Circ.4 (k) USCG Oversight of Safety Management Systems on U.S Flag Vessels, (CVC-WI-003(1)) (l) Maritime Safety Committee / Facilitation Committee Circular 3 "Guidelines on Maritime Cyber Risk Management," MSC-FAL.1/Circ.3 (m) USCG Assistant Commandant for Prevention Policy (CG-5P) Policy Letter 08-16 " Reporting Suspicious Activity and Breaches of Security"				

A. Purpose. Reference (a) calls for Safety Management Systems required under the ISM Code to address cyber risks. This work instruction (WI) provides guidance regarding the U.S. Coast Guard (USCG) commercial vessel compliance program's approach to assessing the cyber risk on vessels to ensure vessels do not pose a risk to the Marine Transportation System (MTS) due to a cyber event.

B. Action. Marine Inspectors (MIs) and Port State Control Officers (PSCOs) should be familiar with reference (b) and use the guidance provided in this WI to evaluate how well a vessel's Safety Management System (SMS) complies with references (a) and (c-f). Additionally, this WI provides guidance to MIs when assessing cyber risk management onboard non-SMS U.S. vessels. Lastly, this WI discusses use of COTP orders and CG-835Vs to control vessels that have been affected by a cyber incident, and responding to a reported or probable cyber incident affecting the seaworthiness of a vessel.

U.S. flagged vessels subject to reference (c) are required to evaluate cyber risk and establish procedures to respond to a cyber-attack as per reference (d). Starting January 1, 2021, all vessels with a Safety Management System (SMS) pursuant to reference (a) should address cybersecurity risk

OpEdge SOLUTIONS

DELIVERING THE OPERATIONAL EDGE

SERVICES

- Program Management and Architecture
- Cybersecurity Maturity Consulting
- Cloud, Infrastructure, and Network Services
- Agile and SecDevOps
- Wireless and Mobility Services
- Integrated Logistics and ERP Consulting

What is the "Operational Edge"?

The mission or business area of responsibility of the operator, agent, warfighter or business user on land, air or sea.

What is Our Role?

We are global leaders and solution architects who transform tactical business processes and simplify information technology to deliver secure, mission-ready solutions to the operational edge.

SOLUTIONS

- Edge Cloud Interconnection
- Edge Security (Coming Soon)
- Edge Analytics (Coming Soon)

Semper Paratus

Questions?