The United States Coast Guard

LESSONS LEARNED IN DEVELOPING CYBERSECURITY FRAMEWORK (CSF) PROFILES WITH INDUSTRY AND THE U.S. COAST GUARD (USCG)

Lessons Learned in Developing CSF Profiles With Industry and USCG

LCDR Brandon Link, USCG
LCDR Josephine Long, USCG
Julie Snyder, NCCoE
David Weitzel, NCCoE

Smart Ports 2018

Topics

10 – Leverage Existing Industry Standards

9 – Be Educational AND Interactive

8 – Have Fun (But with a Purpose)

7 – Leverage Existing Industry Structures

6 – Show Your Work While You Do It

5 – Build on Work You've Already Done

4 – Link It All Together for C-Suite, Managers, Techies

3 – Provide Details for the Techies

2 – Use Industry Led Decision Making (You Have to Live With It)

1 – Make it Actionable

10 - Leverage Existing Technical Standards

Ain't broke, don't fix:

- The NIST Cybersecurity Framework was already 'baked'
- ISO standards are already in use by other members of the CLIA community
- Class Societies have a 300-year history
- CLIA and other organizations/companies/trade groups have well known safety/risk mitigation standards

9 - Be Educational AND Interactive

Workshop Structure

Day 1 –

- Objectives of the Profile Work
- Cybersecurity Framework Overview
- Cybersecurity Framework Profile Development
- Path Forward
- Discussion of Mission Objectives

Day 2 –

- Framework Category Prioritization
- Discussion of Profile Needs

9A - Cybersecurity Framework Overview

Framework Core

Categories and Subcategories

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?

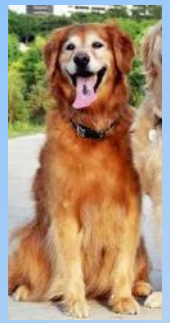
Function	Category	Category Unique ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	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

8 - Have Fun (But with a Purpose)

Big Dog Scale Ranking System

- How important is each Mission Objective?
  - Scale: 1, 3, 5, 8, 13



1 3 5 8 13

7 - Leverage Existing Industry Structures

Trade Associations

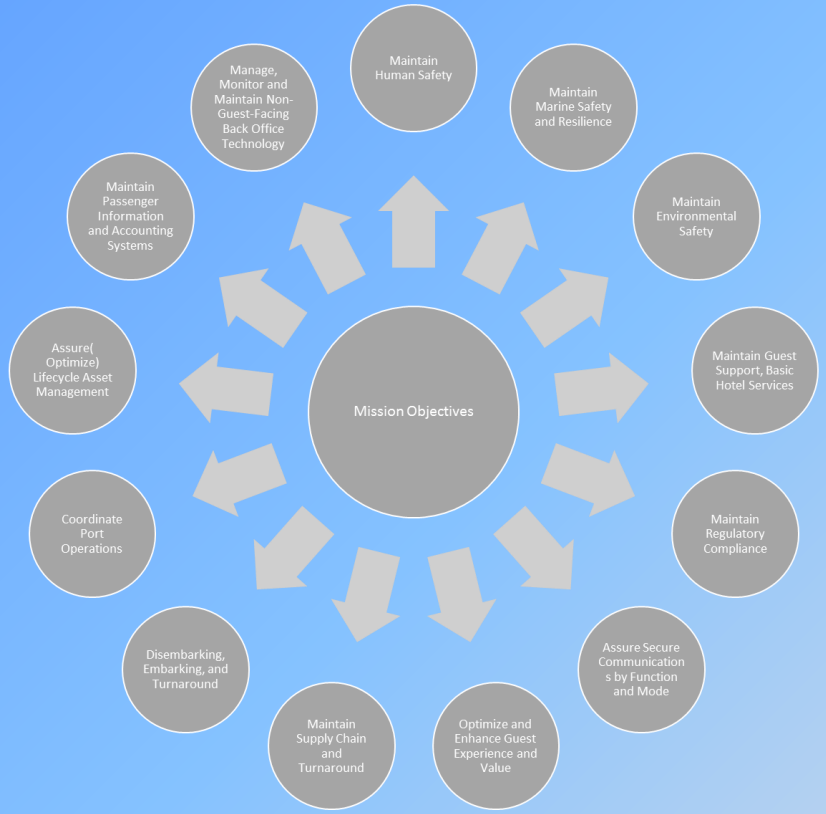
- Cruise Lines International Association (CLIA)
- Passenger Vessel Association (PVA)

Passenger Vessel Operations Profile Mission Objectives

1. Maintain Human Safety
2. Maintain Marine Safety and Resilience
3. Maintain Environmental Safety
4. Maintain Guest Support, Basic Hotel Services
5. Maintain Regulatory Compliance
6. Assure Secure Communications by Function and Mode
7. Optimize and Enhance Guest Experience and Value
8. Maintain Supply Chain and Turnaround
9. Disembarking, Embarking, and Turnaround
10. Coordinate Port Operations
11. Assure (Optimize) Lifecycle Asset Management
12. Maintain Passenger Information and Accounting Systems
13. Manage, Monitor, and Maintain Non-Guest-Facing Back Office Technology

Smart Ports 2018

6 - Show Your Work While You Do It



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 Profi

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

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

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

A profile implements the NIST Cybersecurity Framework, which was developed in
address and manage cybersecurity risk in a cost-effective way based on business
and without placing additional regulatory requirements on businesses. The profile
organizations align the Framework's cybersecurity activities, outcomes, and inform
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. T
comment, download and complete the comment matrix, and email it to HQS-SMB-
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

Mariner Credentialing
Navigation Systems
Operating & Environmental Standards
Ports and Facilities
– Cargo & Facilities
– Domestic Ports
Safety
Standards Evaluation & Development
Uncategorized
Vessel Documentation
Waterways Policy

Passenger Vessel Profile Content Preview

Passenger Vessel Mission Objectives

Table 1. Passenger Vessel Mission Objectives

Mission Objective	Description
1. Maintain Human Safety	Recognizing cybersecurity-effects on process control systems that impact personnel safety. Preventing injury, including loss of life through: Asset Management, Risk Assessment, Access Control, Awareness and Training, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes, Response Planning, Response Communications, Recovery Planning, and Recovery Communications. Organizations should: • account for all personnel on board active equipment • understand scope of operational threats and their impacts to people • manage risks to personnel using a structured process • identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact personnel safety • implement Detect/Respond/Recover activities where cybersecurity adversely affects personnel safety
2.Maintain Marine Safety and Resilience	Preserving systems integrity so that they function as designed and intended throughout their planned life. Prevention of accidents and business impacts through: risk assessment; anomaly detection; asset management; and protective technology. Organizations should: • examine components that can cause failure alone or in combination • design IT and OT integration points to "fail safe"

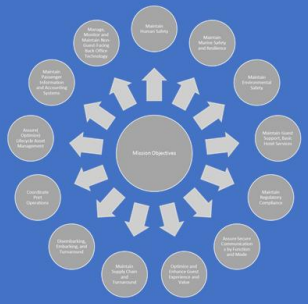
Smart Ports 2018

5 - Build on Work You've Already Done

Smart Ports 2018

4 - Link It All Together for C-Suite, Managers, Techies

Industry Mission Objectives



Cybersecurity Framework

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

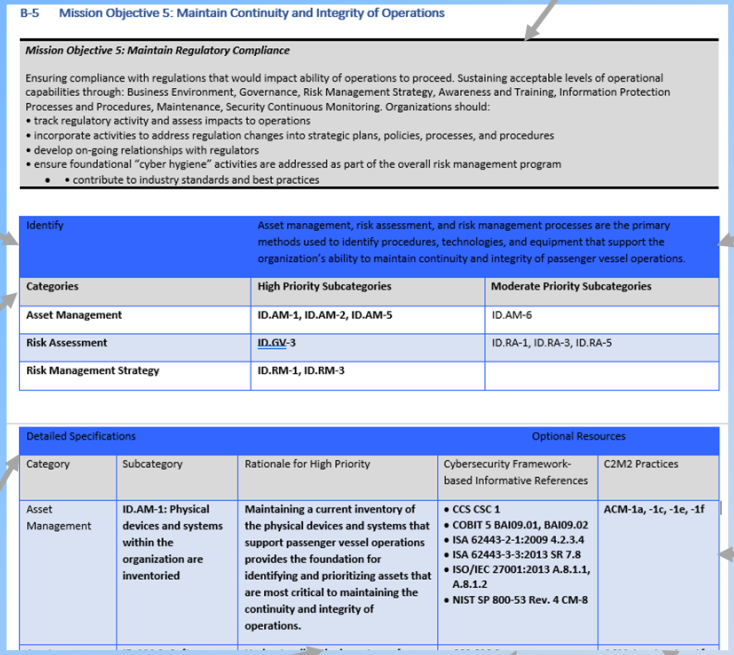
Passenger Vessel CFP

Function	Category	Subcategory	Mission Objectives ●●● – High Priority, ●● – Moderate Priority, ● = Other Implemented Subcategories												
			1	2	3	4	5	6	7	8	9	10	11	12	13
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	•	•	•	••	•••	•	•	••	••	•	•••	•	•
		ID.AM-2: Software platforms and applications within the organization are inventoried	•	•	•	••	•••	•	•	•	•	•	•••	•	•
		ID.AM-3: Organizational communication and data flows are mapped	•	•	•	•	•	•	•	•••	•••	•	•	•	•
		ID.AM-4: External information systems are catalogued	•	•	•	•	•	•	•	•	•	•	•••	•	•
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	•	•••	•	•••	•••	•	•	•••	•••	•	•••	•	•
		ID.AM-6: Cybersecurity roles and responsibilities for the entire	•	•••	•	•••	••	•	•	••	••	•	•	•	•

Smart Ports 2018

3 – Provide Details for the Techies

Text of the Mission Objective



B-5 Mission Objective 5: Maintain Continuity and Integrity of Operations

Mission Objective 5: Maintain Regulatory Compliance

Ensuring compliance with regulations that would impact ability of operations to proceed. Sustaining acceptable levels of operational capabilities through: Business Environment, Governance, Risk Management Strategy, Awareness and Training, Information Protection Processes and Procedures, Maintenance, Security Continuous Monitoring. Organizations should:

- track regulatory activity and assess impacts to operations
- incorporate activities to address regulation changes into strategic plans, policies, processes, and procedures
- develop on-going relationships with regulators
- ensure foundational "cyber hygiene" activities are addressed as part of the overall risk management program
- • contribute to industry standards and best practices

Identify	Asset management, risk assessment, and risk management processes are the primary methods used to identify procedures, technologies, and equipment that support the organization's ability to maintain continuity and integrity of passenger vessel operations.	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Asset Management	**ID.AM-1, ID.AM-2, ID.AM-5**	ID.AM-6
Risk Assessment	**ID.GV-3**	ID.RA-1, ID.RA-3, ID.RA-5
Risk Management Strategy	**ID.RM-1, ID.RM-3**	

Detailed Specifications			Optional Resources	
Category	Subcategory	Rationale for High Priority	Cybersecurity Framework-based Informative References	C2M2 Practices
Asset Management	**ID.AM-1: Physical devices and systems within the organization are inventoried**	**Maintaining a current inventory of the physical devices and systems that support passenger vessel operations provides the foundation for identifying and prioritizing assets that are most critical to maintaining the continuity and integrity of operations.**	• **CCS CSC 1** • **COBIT 5 BAI09.01, BAI09.02** • **ISA 62443-2-1:2009 4.2.3.4** • **ISA 62443-3-3:2013 SR 7.8** • **ISO/IEC 27001:2013 A.8.1.1, A.8.1.2** • **NIST SP 800-53 Rev. 4 CM-8**	**ACM-1a, -1c, -1e, -1f**

Cybersecurity Framework Function, section color-coded to align with Framework format

Summary table of Subcategory specifications for each Cybersecurity Framework Function in the context of the Mission Objective, broken out between High and Moderate priorities

Detailed table of Subcategory specifications for each Cybersecurity Framework Function in the context of the Mission Objective

General Industry context for the Cybersecurity Framework Function

Cybersecurity Framework Category and Subcategory, color-coded rows with bold font indicate "High Priority" Subcategories that should be addressed first, remaining rows are "Moderate Priority" Subcategories that should be addressed prior to addressing all remaining relevant "Other Implemented Subcategories".

Industry context that describes the reasoning behind designating certain Subcategories as High Priority

Non-exhaustive list of informative references, based on the Cybersecurity Framework (optional)

Crosswalk of related C2M2 practices (optional)

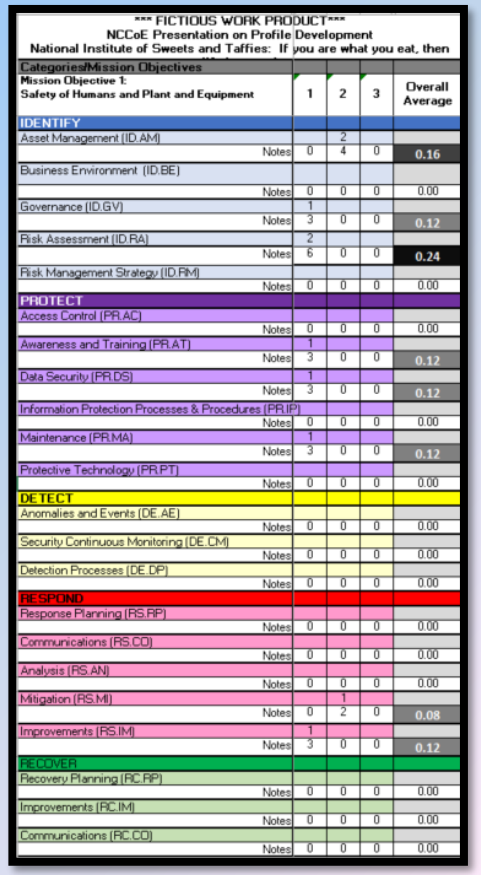
2 – Use Industry Led Decision Making

(You Have to Live with It)

Ranking of Top 3 Categories that Support Mission Objectives, sample analysis:

Highest Priority	Moderate Priority	Low Priority
▸ Risk Assessment (ID.RA)	▸ Asset Management (ID.AM)	▸ Governance (ID.GV) ▸ Awareness and Training (PR.AT) ▸ Data Security (PR.DS) ▸ Maintenance (PR.MA) ▸ Respond/Mitigation (RS.MI) ▸ Respond/Improvements (RS.IM)

- These would be where we put attention for identifying priority Subcategories in the Profile.
- Remaining Categories and Subcategories would be reviewed by each organization applying to Profile for relevance, too.



*** FICTIOUS WORK PRODUCT***
NCCoE Presentation on Profile Development
National Institute of Sweets and Taffies: If you are what you eat, then

Categories/Mission Objectives Mission Objective 1: Safety of Humans and Plant and Equipment	1	2	3	Overall Average
IDENTIFY				
Asset Management (ID.AM)		2		
Notes:	0	4	0	0.16
Business Environment (ID.BE)				
Notes:	0	0	0	0.00
Governance (ID.GV)	1			
Notes:	3	0	0	0.12
Risk Assessment (ID.RA)	2			
Notes:	6	0	0	0.24
Risk Management Strategy (ID.RM)				
Notes:	0	0	0	0.00
PROTECT				
Access Control (PR.AC)				
Notes:	0	0	0	0.00
Awareness and Training (PR.AT)	1			
Notes:	3	0	0	0.12
Data Security (PR.DS)	1			
Notes:	3	0	0	0.12
Information Protection Processes & Procedures (PR.IP)				
Notes:	0	0	0	0.00
Maintenance (PR.MA)	1			
Notes:	3	0	0	0.12
Protective Technology (PR.PT)				
Notes:	0	0	0	0.00
DETECT				
Anomalies and Events (DE.AE)				
Notes:	0	0	0	0.00
Security Continuous Monitoring (DE.CM)				
Notes:	0	0	0	0.00
Detection Processes (DE.DP)				
Notes:	0	0	0	0.00
RESPOND				
Response Planning (RS.RP)				
Notes:	0	0	0	0.00
Communications (RS.CO)				
Notes:	0	0	0	0.00
Analysis (RS.AN)				
Notes:	0	0	0	0.00
Mitigation (RS.MI)		1		
Notes:	0	2	0	0.08
Improvements (RS.IM)	1			
Notes:	3	0	0	0.12
RECOVER				
Recovery Planning (RC.RP)				
Notes:	0	0	0	0.00
Improvements (RC.IM)				
Notes:	0	0	0	0.00
Communications (RC.CO)				
Notes:	0	0	0	0.00

1 – Make the Results Actionable

What You Can Do with a Profile

Resource and Budget Decisioning

Sub-category	Priority	Gaps	Year 1 Activities	Year 2 Activities
1	moderate	small		X
2	high	large	X	
3	moderate	medium	X	
…	…	…		
98	moderate	none		reassess

…and supports on-going operational decisions, too.

LCDR Brandon Link, USCG
Brandon.M.Link@uscg.mil

Julie Snyder, CIPM, CIPT, CIPP/G/US
jsnyder@mitre.org

David Weitzel, M.S., J.D., CIPP/G/US
dweitzel@mitre.org

Maritime Commons Blog
http://mariners.coastguard.dodlive.mil/

CG-FAC
http://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/cgfac/

NCCoE
https://nccoe.nist.gov/