ARF Cybersecurity Program

Cyberinfrastructure Working Group
ciwg@unols.org
RVTEC 2022-11-01

Presentation Overview

- About CIWG
- CIWG Activities
- Agencies
- Regulations
- U.S. ARF as an NSF Major Facility and Cybersecurity Responsibilities
- Research SOC Services

About CIWG

Following the Fall 2019 ARF/Trusted CI Cybersecurity Engagement UCSD/SCRIPPS coordinated an ad hoc group of ~40 ARF stakeholders who currently meet bi-monthly to advance fleetwide cybersecurity compliance efforts.

As of April 2022, every other CIWG meeting is focused on Operational Cybersecurity considerations across ARF, while the remaining meetings are reserved for more technical discussions.

ARF Cyberinfrastructure Working Group Activities

CIWG has been working to understand complex and evolving cybersecurity regulatory requirements.

CIWG originated out of RVTEC however it is Vessel Operations which is responsible for the regulatory compliance aspects of Cybersecurity.

- 2019 - Trusted CI / ARF Engagement and subsequent report
- 2020 - Reviewed options for meeting the IMO 2021 CRMP deadline
- 2021 - Contracted with Peregrine to meet new IMO cybersecurity guidelines being enforced through ABS/USCG inspections
- 2022 - Contracted with ResearchSOC to manage Cybersecurity Program for the ARF as a NSF Major Facility

Agencies

INTERNATIONAL MARITIME ORGANIZATION

In response to addressing Maritime cyber risk, the IMO has issued MSC-FAL.1/Circ.3 Guidelines for managing cyber risk and adopted Resolution MSC.428(98) in June 2017 which requires the addition of a **Cyber Risk Management Plan (CRMP) to vessel SMS documents by January 1, 2021**. Based on the BIMCO: *The Guidelines on Cyber Security Onboard Ships* and the IMO International Safety Management (ISM) Code.

United States Coast Guard
U.S. Department of Homeland Security

In 2021 the USCG released the USCG Cyber Strategic Outlook, and in April 2022 released a Marine Safety Bulletin which references the CISA Shields Up website as guidance for all organizations to follow.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA is a U.S. Government Cybersecurity resource, providing guidance and notification related to cyber threats for U.S. Government Agencies.

Oversight of Navy owned vessels with tighter cybersecurity controls.

U.S. Department of Defense

OUSD(A&S), DoD, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC) developed the Cybersecurity Maturity Model Certification v2 (CMMC) framework.

National Science Foundation

The NSF Major Facilities Guide, section 6.3 Guidelines for Cyber-security of NFS's Major Facilities outline cybersecurity requirements for NSF major facilities.

U.S. Academic Research Fleet
Cyberinfrastructure Working Group
ciwg@unols.org

ResearchSOC

Regulations

Agency - Regulation	Documentation Framework	Responsible Party	Controls
IMO - MSC-FAL.1/Circ.3 (ABS & USCG Inspections) USCG MSIB 02-22	SMS / CRMP	Each Vessel Operator (Marine Sup)	IMO Annex 2 (tmpl) ● 5 Processes ● 23 Controls
DoD - DFARS Case 2019-D041	CMMC 2.0 SPRS Registration NIST SP 800-171 NIST SP 800-172	Each University or Institution (CISO) Cyber Information Security Officer	CMMC 2.0 ● Level 1 - 17 Controls with 59 Objectives (tmpl) ● Level 2 - 110 Controls ● Level 3 - 110+ TBD
NSF Major Facility Guide section 6.3	Trusted CI	ARF - ResearchSOC (RSOC CISO)	Major Facility Guide section 6.3 Trusted CI ● 4 Pillars ● 16 Musts CIS Controls

Cyber Risk Management Plan (CRMP)

In response to addressing Maritime cyber risk[1], the IMO has issued MSC-FAL.1/Circ.3[2] Guidelines for managing cyber risk and adopted Resolution MSC.428(98)[3] in June 2017 which requires the addition of a Cyber Risk Management Plan (CRMP) to vessel SMS documents by January 1, 2021. Based on the BIMCO: *The Guidelines on Cyber Security Onboard Ships*[4] and the IMO International Safety Management (ISM) Code[5].

- As of Jan 1, 2021, it is the responsibility of each Vessel Operator to maintain an accurate and up to date Cyber Risk Management Plan (CRMP) as part of the Vessels Safety Management System (SMS) documentation.
- ARF vessels have been being on CRMP since 2021.
- Research SOC is developing CRMP templates for ARF that can be adopted by operating institutions.

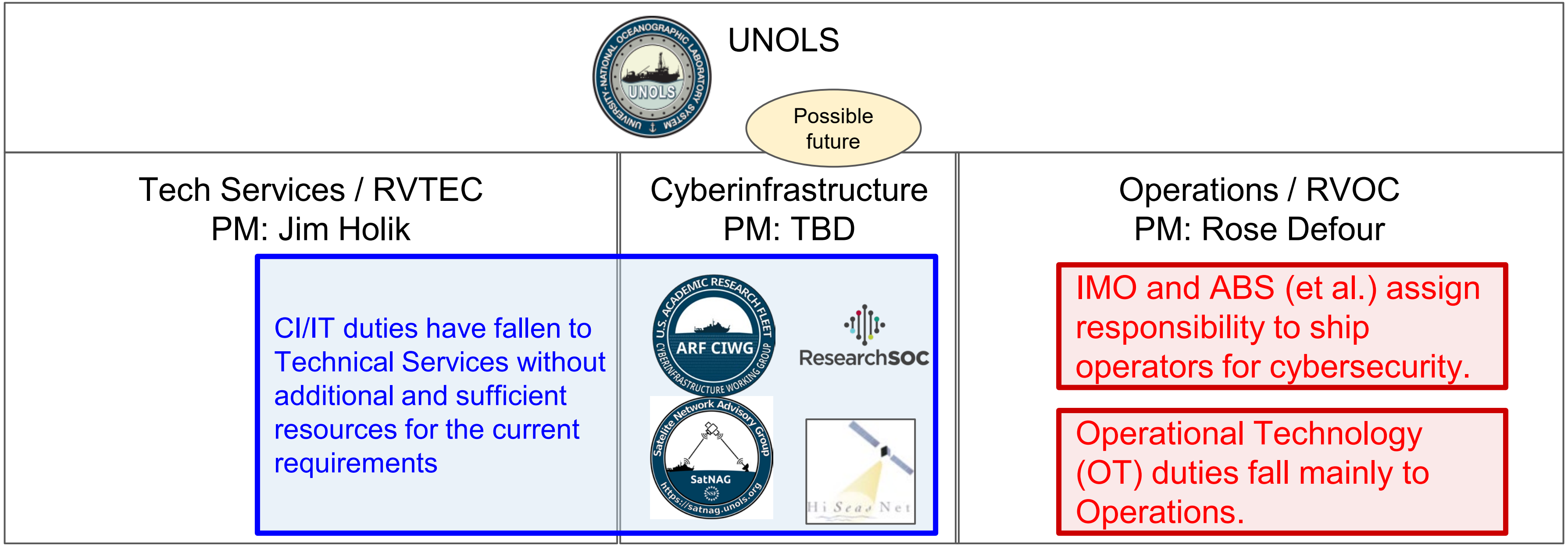
Academic Research Fleet as a Major Facility

Major Facilities (MF) represent some of the largest National Science Foundation (NSF) investments, producing scientific advances and discoveries at scale; the cyber infrastructure (CI) and cyber security (CS) are essential to facilitate these operations and scientific research missions or each MF. **It is essential that the facility science is transformed (not limited) by the CI**.

The needs of each MF science should drive the CI needs. This will influence how many things are approached and will change over time as the science evolves. Defining the desired outcome and developing those tools will help MF realize these CI/CS goals.

U.S. Academic Research Fleet

An NSF Major Facility



UNOLS

Possible future

Tech Services / RVTEC
PM: Jim Holik

Cyberinfrastructure
PM: TBD

Operations / RVOC
PM: Rose Defour

CI/IT duties have fallen to Technical Services without additional and sufficient resources for the current requirements

IMO and ABS (et al.) assign responsibility to ship operators for cybersecurity.

Operational Technology (OT) duties fall mainly to Operations.

Research Security Operation Center

https://researchsoc.iu.edu/

The NSF-funded ResearchSOC helps make scientific computing resilient to cyberattacks and capable of supporting trustworthy, productive research through operational cybersecurity services, training, and information sharing necessary to a community as unique and variable as research and education (R&E).

ARF ResearchSOC Services

- Starting Jan 2022
- Virtual CISO - Ryan Kiser (Indiana University)
- OmniSOC Traffic Monitoring
- Vulnerability Scanning
- STINGAR HoneyPots
- Virtual Security Team
- RedPhone - Urgent Response Service
- ARF CRMP Templates

U.S. Academic Research Fleet
Cyberinfrastructure Working Group
ciwg@unols.org

ARF Cybersecurity Program

Cyberinfrastructure Working Group
ciwg@unols.org
RVTEC 2022-11-01

Additional Reference Slides

U.S. Academic Research Fleet
Cyberinfrastructure Working Group
ciwg@unols.org

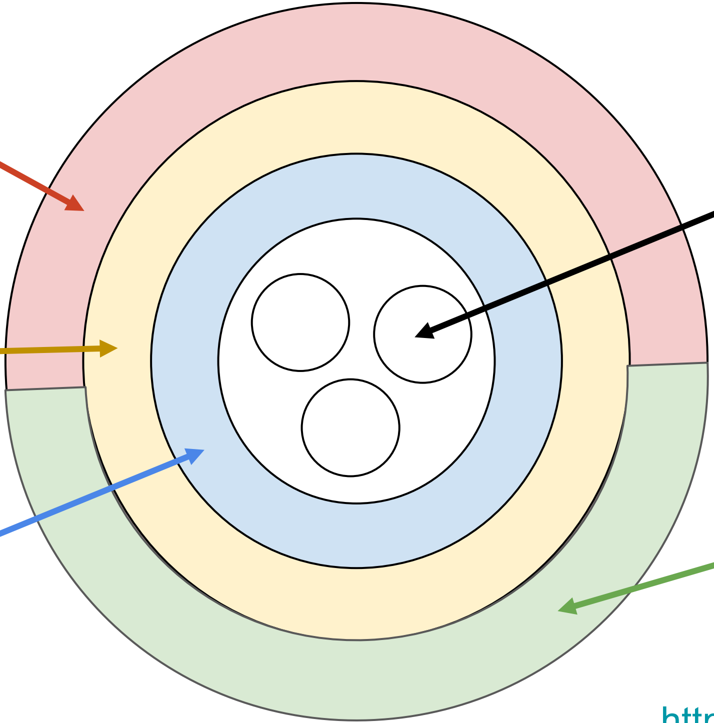
IT vs OT

IT Security Zones
(~Tech Services)

Transient Systems (WiFi)
- Science Party
- Crew
- Contractors

Shared CI
- DNS
- File Shares
- Web
- Printers

Science / DAS
- Data Storage
- Instrumentation



OT Security Zones
(~Operations)

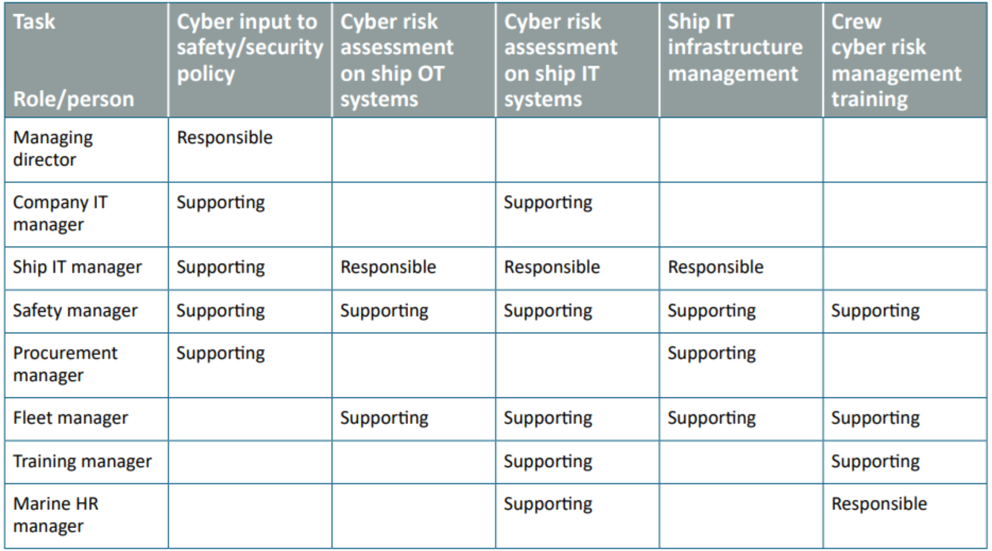
Isolated (AirGap) Networks
- Eng
- Bridge
- CCTV

Operational Technology
- Crew Kiosks

https://zenodo.org/record/6828675

U.S. Academic Research Fleet
Cyberinfrastructure Working Group
ciwg@unols.org

CRMP: Roles and Responsibilities



Task Role/person	Cyber input to safety/security policy	Cyber risk assessment on ship OT systems	Cyber risk assessment on ship IT systems	Ship IT infrastructure management	Crew cyber risk management training
Managing director	Responsible				
Company IT manager	Supporting		Supporting		
Ship IT manager	Supporting	Responsible	Responsible	Responsible	
Safety manager	Supporting	Supporting	Supporting	Supporting	Supporting
Procurement manager	Supporting			Supporting	
Fleet manager		Supporting	Supporting	Supporting	Supporting
Training manager			Supporting		Supporting
Marine HR manager			Supporting		Responsible

Figure 3: Example (non-exhaustive) of mapping roles, responsibilities, and tasks in a matrix. Job titles and associated job scope and responsibilities will vary from company to company. IT and OT responsible persons need to align and coordinate the company's cyber risk management strategy.

RVOC Cybersecurity Action Items

1. Assign 3-5 RVOC representatives to participate in monthly CIWG meetings
2. Reading (everyone)
    a. The Guidelines on Cyber Security Onboard Ships
    b. Review CIWG IMO Annex 2 Checklist
    c. Review CIWG CMMC 2.0 Level 1 Checklist
    d. Your vessels SMS / CRMP Documents
3. Assign Cybersecurity Roles and Responsibilities (Page 7) for your vessel
4. Complete CIWG IMO Annex 2 Checklist 23 action items for your vessels CRMP
5. Contact your institution CISO regarding SPRS Registration and CMMC 2.0 compliance.
6. (Optional) Attend Trusted CI Cybersecurity Summit in October

U.S. Academic Research Fleet
Cyberinfrastructure Working Group
ciwg@unols.org

CI/IT Staffing Levels

Departments onboard vessels have teams of crew, and a relief crew to provide business continuity and cross training.

- Bridge Crew
- Deck Crew
- Engineering
- Galley
- Marine Techs

Most vessels do not have dedicated CI/IT positions and often depend on oversubscribed Marine Techs for CI/IT needs.

Additional Cybersecurity workload will require additional staffing resources.

Tech Services can provide a supporting role for IT and CI but cannot address Operational Tech (OT) Cybersecurity workloads.

There are not berths available for onboard IT/CI staff. The fleet may need to consider a hybrid model for shoreside IT/CI staff and/or increase levels of Marine Tech staffing to address the oceans of technical debt and cybersecurity related maintenance activities we are now required to perform.

Academic Research Fleet

- Vessels are remote research platforms
- Operated by different institutions
- Low bandwidth/ high latency
  - Not all vessels have the same connectivity
  - Some blockage zones depending on heading and/or location
- CI/CS rules governed by multiple entities
  - Owner Entity
  - Operator Institution
  - PI Institution
  - Grant Funding Institution

The Guidelines on Cyber Security Onboard Ships

https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf

Provides guidance for CRMP

- ~50 Pages and is easy to read
- Industry Best Practices for Cybersecurity
- Vessel based considerations
- Distinguishing IT from OT
- Identify > Protect > Detect > Respond > Recover
- Roles and Responsibilities
- Annex 2 - Cybersecurity Checklist / Controls

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

Produced and supported by

BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC)

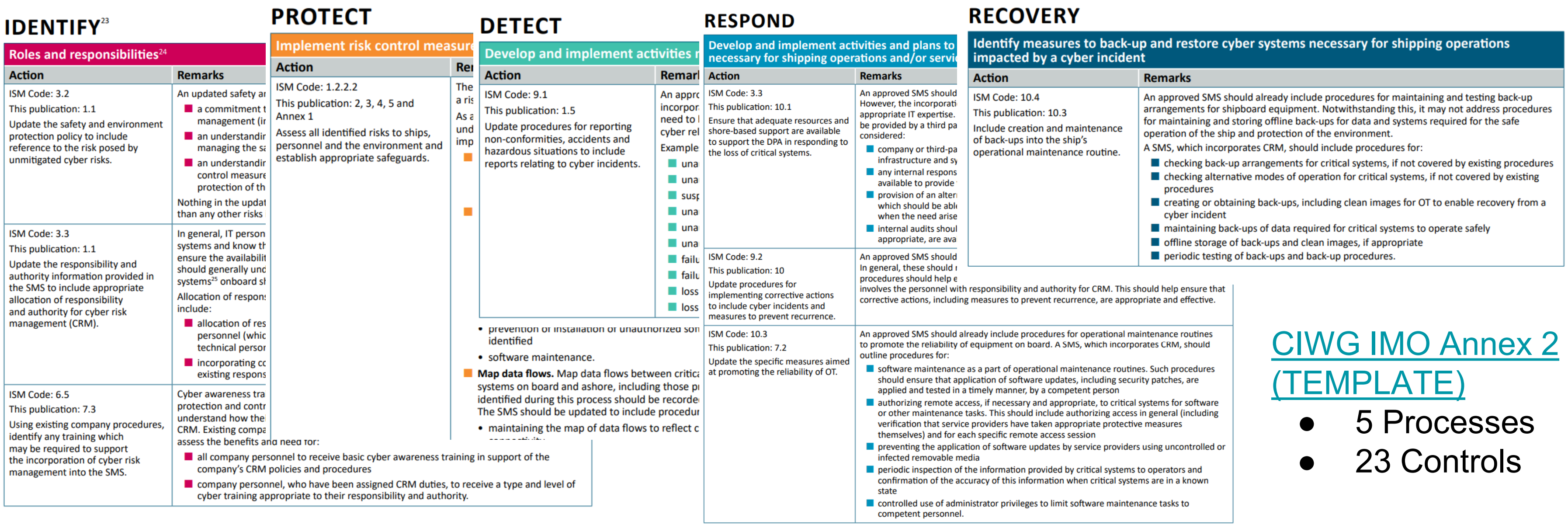
v4

IMO: MSC-FAL.1/Circ.3

In response to addressing Maritime cyber risk, the IMO has issued MSC-FAL.1/Circ.3 Guidelines for managing cyber risk and adopted Resolution MSC.428(98) in June 2017 which requires the addition of a **Cyber Risk Management Plan (CRMP) to vessel SMS documents by January 1, 2021**. Based on the BIMCO: *The Guidelines on Cyber Security Onboard Ships* and the IMO International Safety Management (ISM) Code.

CRMP: Annex II

Cybersecurity Checklist / Controls



IDENTIFY[23]

Roles and responsibilities[24]

Action	Remarks
ISM Code: 3.2 This publication: 1.1 Update the safety and environment protection policy to include reference to the risk posed by unmitigated cyber risks.	An updated safety ar ■ a commitment t management (ir ■ an understandir managing the sa ■ an understandir control measure protection of th Nothing in the updat than any other risks
ISM Code: 3.3 This publication: 1.1 Update the responsibility and authority information provided in the SMS to include appropriate allocation of responsibility and authority for cyber risk management (CRM).	In general, IT person systems and know th ensure the availabilit should generally und systems[25] onboard sh Allocation of respon: include: ■ allocation of res personnel (whic technical persor ■ incorporating cc existing respons
ISM Code: 6.5 This publication: 7.3 Using existing company procedures, identify any training which may be required to support the incorporation of cyber risk management into the SMS.	Cyber awareness tra protection and contr understand how the CRM. Existing compa assess the benefits and need for: ■ all company personnel to receive basic cyber awareness training in support of the company's CRM policies and procedures ■ company personnel, who have been assigned CRM duties, to receive a type and level of cyber training appropriate to their responsibility and authority.

PROTECT

Implement risk control measure

Action	Re
ISM Code: 1.2.2.2 This publication: 2, 3, 4, 5 and Annex 1 Assess all identified risks to ships, personnel and the environment and establish appropriate safeguards.	The a ris As a und imp ■ ■

DETECT

Develop and implement activities n

Action	Remarl
ISM Code: 9.1 This publication: 1.5 Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber incidents.	An appro incorpor need to l cyber rel Example ■ una ■ una ■ susp ■ una ■ una ■ una ■ failu ■ failu ■ loss ■ loss

- prevention of installation of unauthorized sof identified
- software maintenance.

■ **Map data flows.** Map data flows between critica systems on board and ashore, including those pr identified during this process should be recorde The SMS should be updated to include procedur

- maintaining the map of data flows to reflect c connectivity

RESPOND

Develop and implement activities and plans to necessary for shipping operations and/or servic

Action	Remarks
ISM Code: 3.3 This publication: 10.1 Ensure that adequate resources and shore-based support are available to support the DPA in responding to the loss of critical systems.	An approved SMS should However, the incorporati appropriate IT expertise. be provided by a third pa considered: ■ company or third-pa infrastructure and sy ■ any internal respons available to provide ■ provision of an alter which should be able when the need arise ■ internal audits shoul appropriate, are avai
ISM Code: 9.2 This publication: 10 Update procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence.	An approved SMS should In general, these should r procedures should help e involves the personnel with responsibility and authority for CRM. This should help ensure that corrective actions, including measures to prevent recurrence, are appropriate and effective.
ISM Code: 10.3 This publication: 7.2 Update the specific measures aimed at promoting the reliability of OT.	An approved SMS should already include procedures for operational maintenance routines to promote the reliability of equipment on board. A SMS, which incorporates CRM, should outline procedures for: ■ software maintenance as a part of operational maintenance routines. Such procedures should ensure that application of software updates, including security patches, are applied and tested in a timely manner, by a competent person ■ authorizing remote access, if necessary and appropriate, to critical systems for software or other maintenance tasks. This should include authorizing access in general (including verification that service providers have taken appropriate protective measures themselves) and for each specific remote access session ■ preventing the application of software updates by service providers using uncontrolled or infected removable media ■ periodic inspection of the information provided by critical systems to operators and confirmation of the accuracy of this information when critical systems are in a known state ■ controlled use of administrator privileges to limit software maintenance tasks to competent personnel.

RECOVERY

Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident

Action	Remarks
ISM Code: 10.4 This publication: 10.3 Include creation and maintenance of back-ups into the ship's operational maintenance routine.	An approved SMS should already include procedures for maintaining and testing back-up arrangements for shipboard equipment. Notwithstanding this, it may not address procedures for maintaining and storing offline back-ups for data and systems required for the safe operation of the ship and protection of the environment. A SMS, which incorporates CRM, should include procedures for: ■ checking back-up arrangements for critical systems, if not covered by existing procedures ■ checking alternative modes of operation for critical systems, if not covered by existing procedures ■ creating or obtaining back-ups, including clean images for OT to enable recovery from a cyber incident ■ maintaining back-ups of data required for critical systems to operate safely ■ offline storage of back-ups and clean images, if appropriate ■ periodic testing of back-ups and back-up procedures.

CIWG IMO Annex 2 (TEMPLATE)

- 5 Processes
- 23 Controls

U.S. Academic Research Fleet
Cyberinfrastructure Working Group
ciwg@unols.org

Executive Summary

1. IMO and ABS (et al) assign responsibility to ship operators for cybersecurity. We need engagement from all stakeholders to establish a functional model for dealing with these new regulations
2. New work requires new resources
3. Tech Services is interested in a supporting role
4. CIWG is an NSF working group engaged in finding ways forward regarding cyberinfrastructure and cybersecurity, CIWG is also directly working with ResearchSOC on cybersecurity planning and policies
5. We want you involved. We have some homework for you: CIWG needs input from Ship Operators, Captains and Tech Managers

IMO: SMS & CRMP

Cyber Risk Management Plan (CRMP)

- As of Jan 1, 2021, the CRMP must be included as part of a vessels Safety Management System documentation.
- It is each operating institution’s responsibility to maintain their SMS and CRMP documentation.
- In 2021: the ARF contracted with Peregrine Technical Solutions to assist each UNOLS operator develop baseline CRMP documentation and pass ABS inspections in 2021.
- In 2022: the ARF has contracted with ResearchSOC to provide long term administration of a fleetwide Major Facility Cybersecurity Program.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Shields Up

https://www.cisa.gov/shields-up

Empower Chief Information Security Officers (CISO): In nearly every organization, security improvements are weighed against cost and operational risks to the business. In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company, and ensure that the entire organization understands that security investments are a top priority in the immediate term.

Lower Reporting Thresholds: Every organization should have documented thresholds for reporting potential cyber incidents to senior management and to the U.S. government. In this heightened threat environment, these thresholds should be significantly lower than normal. Senior management should establish an expectation that any indications of malicious cyber activity, even if blocked by security controls, should be reported to **report@cisa.gov**. Lowering thresholds will ensure we are able to immediately identify an issue and help protect against further attack or victims.

Participate in a Test of Response Plans: Cyber incident response plans should include not only your security and IT teams, but also senior business leadership and Board members. If you’ve not already done, senior management should participate in a tabletop exercise to ensure familiarity with how your organization will manage a major cyber incident, to not only your company but also companies within your supply chain.

Focus on Continuity: Recognizing finite resources, investments in security and resilience should be focused on those systems supporting critical business functions. Senior management should ensure that such systems have been identified and that continuity tests have been conducted to ensure that critical business functions can remain available subsequent to a cyber intrusion.

Plan for the Worst: While the U.S. government does not have credible information regarding specific threats to the U.S. homeland, organizations should plan for a worst-case scenario. Senior management should ensure that exigent measures can be taken to protect your organization’s most critical assets in case of an intrusion, including disconnecting high-impact parts of the network if necessary.

ABS

https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/251_cybersafety_2021/cybersafety-v2-cybersecurity-guide-feb21.pdf

ABS Cybersecurity Implementation for the Marine and Offshore Industries

Definitions and Abbreviations -> *Cybersecurity Representative*

A chartered organizational entity or person responsible for implementation and maintenance of a cybersecurity risk management program and/or system(s). The ashore person in charge of this office may be referred to as the Chief Information Officer (CIO), Cyber Security Representative or Cybersecurity Designated Person Ashore (DPA). The onboard person responsible for cybersecurity may be referred to as the Electro-Technical Officer (ETO) or the Chief Engineer.

CRMP: IT vs OT

1.4 Differences between IT and OT systems

Whereas IT systems manage data and support business functions, OT is the hardware and software that directly monitors/controls physical devices and processes and as such are an integral part of the ship and must function independently of the IT systems onboard. The systems can, however, be connected to the IT network for performance monitoring, remote support etc. Such systems are sometimes referred to as belonging to the Industrial Internet of Things (IIOT). In such cases, it must be ensured that the interface is sufficiently guarded by a firewall as a minimum and potential THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS V4 Cyber security and risk management 8 vulnerabilities in the OT systems are not exposed in the IT network. This is important because it is not always possible or feasible to ensure a proper patch level in OT systems.

IT covers the spectrum of technologies for information processing, including software, hardware, and communication technologies. Traditionally OT and IT have been separated, but with the internet, OT and IT are coming closer as historically stand-alone systems are becoming integrated. Disruption of the operation of OT systems may impose significant risk to the safety of onboard personnel, cargo, damage to the marine environment and impede the ship's operation. Likewise, failure of certain IT systems, eg lack of immediate access to dangerous goods manifest, could also result in hazardous situations. For example, in situations where a container aboard ship is on fire, information about the contents of adjacent containers is critical for proper firefighting.

There may be important differences between who handles the purchase and management of the OT systems versus IT systems on a ship. IT managers are not usually involved in the purchase of OT systems and may or may not have a thorough understanding of cyber security. The purchase of such systems should involve someone, who knows about the impact on the onboard systems but will most probably only have limited knowledge of software and cyber risk management. It is therefore important to have a dialogue with an individual knowledgeable of cyber security to ensure that cyber risks are considered during the OT purchasing process. Updating of OT software requires a thorough compatibility check and class approval as opposed to IT software, which is normally updated routinely. To obtain an overview of potential challenges and to help establish the necessary policy and procedures for software maintenance, it can be an advantage for the party responsible for cyber security on board the ship to have an inventory of OT systems.

DoD - CMMC

- DFARS Case 2019-D041 - Interim Rule
- SPRS Registration - **Applies at an institution level for anyone seeking DoD funding.**
- CMMC 2.0

CMMC 2.0 L1

- CMMC 2.0 Level 1 Assessment Guide
- CIWG CMMC 2.0 L1 Checklist (TEMPLATE)
- 17 Controls - 59 Assessment Objectives

University will not be able to renew DoD contracts if not CMMC compliant.

CMMC 2.0 L2

- CMMC 2.0 Level 2 Assessment Guide
- 110 Controls

What is needed from Operators?

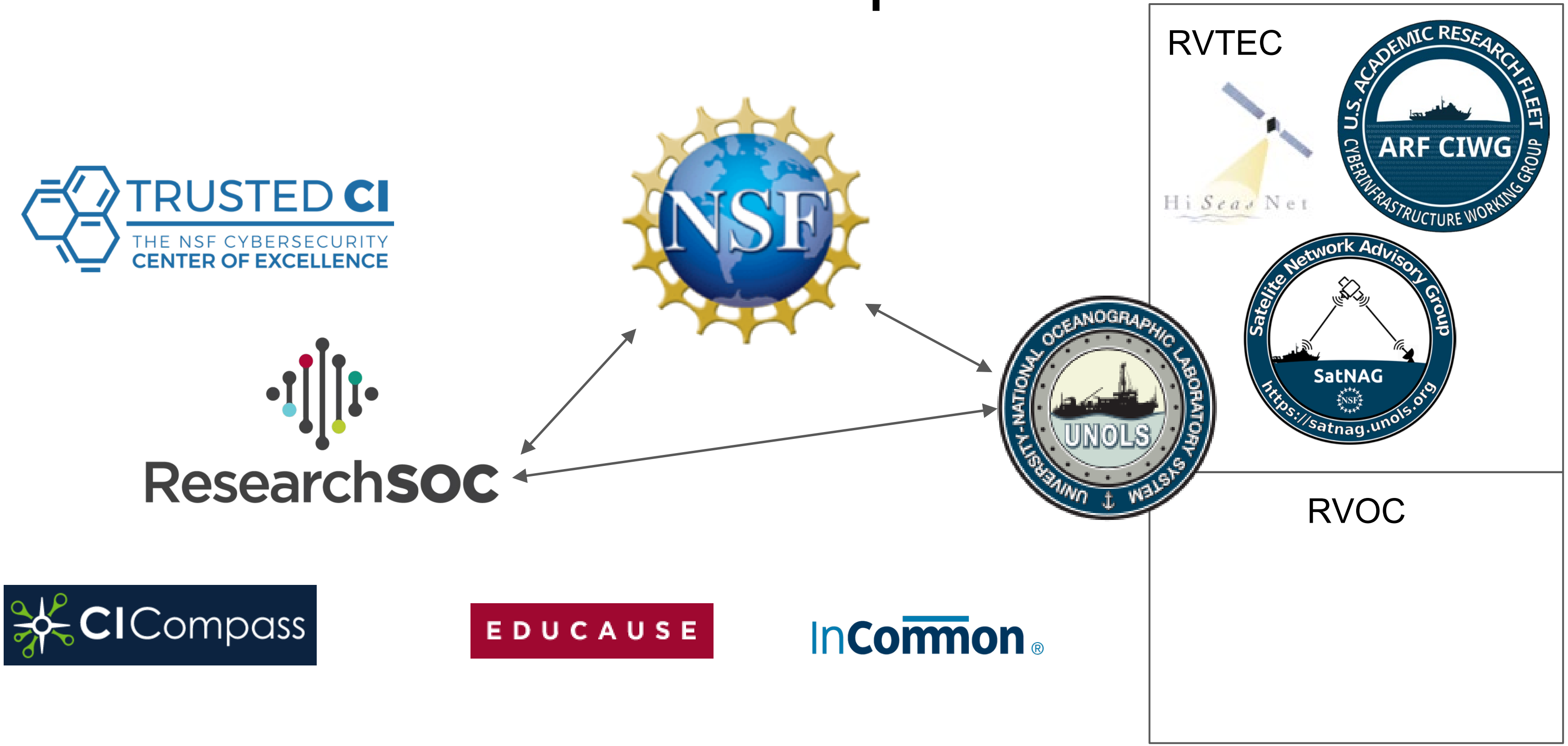
ARF / IMO / ResearchSOC

- Assign Roles and Responsibilities
- Maintain an accurate and up to date CRMP
- Annex 2: Complete and maintain compliance of all controls
  - CyberSec Training for all Crew and Science Parties
  - Asset Management for all devices
  - Keep software up to date
  - Maintain per person identities and authorization
- Regular engagement and representation in CIWG cybersecurity efforts

DoD / CMMC 2.0

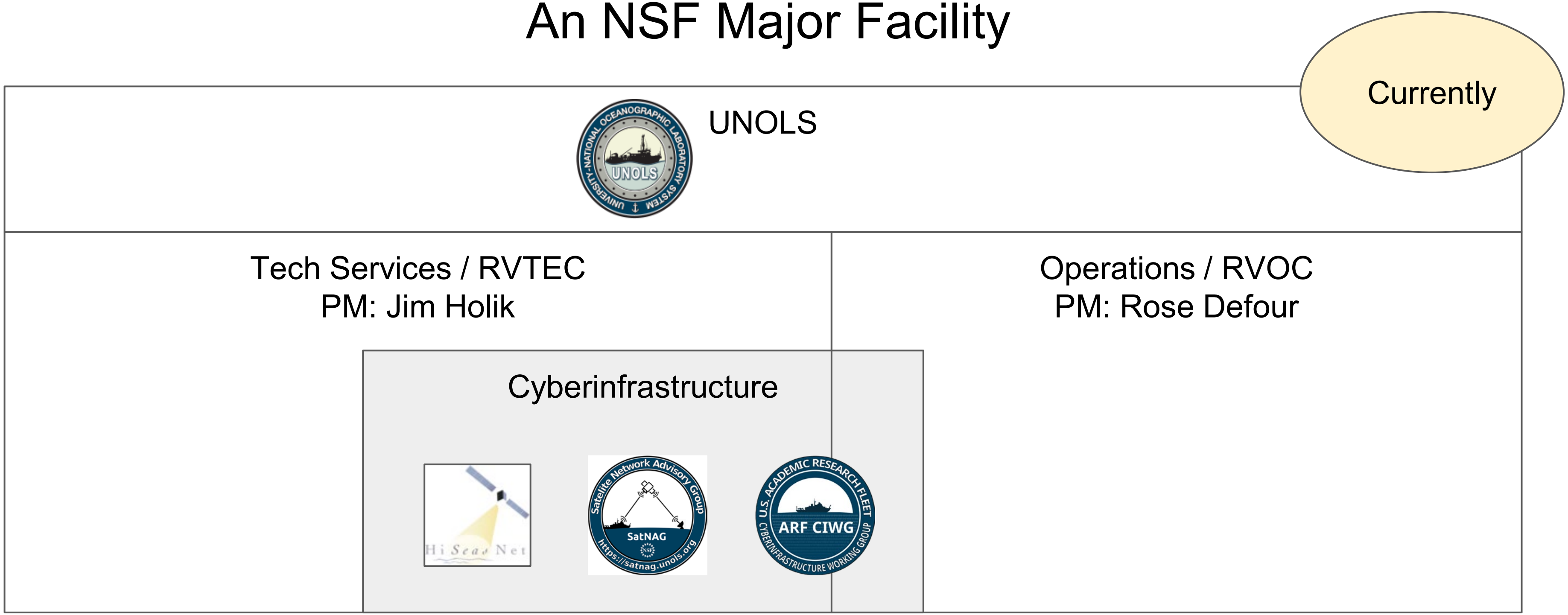
- At your University / Institution
- For Navy owned vessels and other DoD research funding.
- SPRS Registration
- CMMC 2.0: Complete and maintain compliance with all controls.

Partnerships


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
NSF
ResearchSOC
UNIVERSITY-NATIONAL OCEANOGRAPHIC LABORATORY SYSTEM
UNOLS
RVTEC
HiSeasNet
U.S. ACADEMIC RESEARCH FLEET CYBERINFRASTRUCTURE WORKING GROUP
ARF CIWG
Satellite Network Advisory Group
SatNAG
https://satnag.unols.org
RVOC
CICompass
EDUCAUSE
InCommon®

U.S. Academic Research Fleet

An NSF Major Facility



Currently

UNOLS

Tech Services / RVTEC
PM: Jim Holik

Operations / RVOC
PM: Rose Defour

Cyberinfrastructure

HiSeasNet
Satellite Network Advisory Group
SatNAG
https://satnag.unols.org
U.S. Academic Research Fleet
ARF CIWG
Cyberinfrastructure Working Group

U.S. Academic Research Fleet
Cyberinfrastructure Working Group
ciwg@unols.org

ResearchSOC

Frameworks

The NIST Cybersecurity Framework is an older framework which is widely used, and frequently referenced in cybersecurity circle.

U.S. Department of Defense

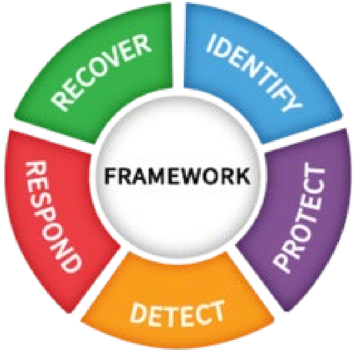
OUSD(A&S), working with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry to develop the Cybersecurity Maturity Model Certification v2 (CMMC) framework.

The Trusted CI Framework is a minimum standard for cybersecurity programs. In response to cybersecurity guidance focused narrowly on cybersecurity controls, the Trusted CI Framework provides a more holistic and mission-focused standard for managing cybersecurity.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

A maritime working group develop The Guidelines on Cyber Security Onboard Ships with a focus on maritime specific considerations for cybersecurity. This document is widely referenced by IMO, ABS and other regulators.

Frameworks



RECOVER

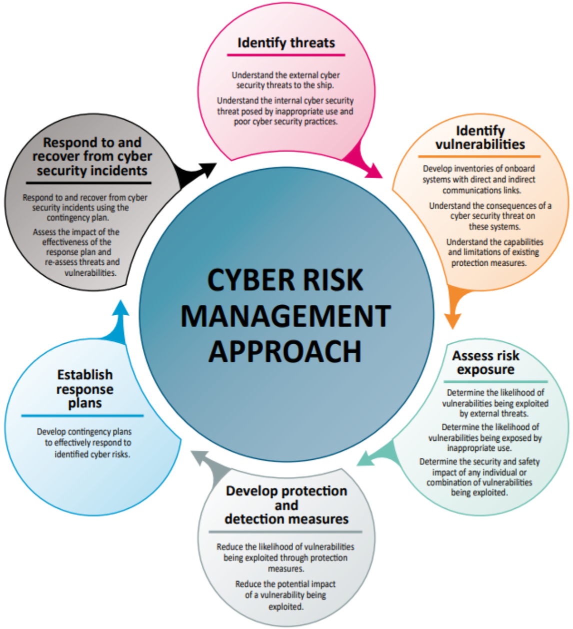
IDENTIFY

PROTECT

DETECT

RESPOND

FRAMEWORK



CYBER RISK MANAGEMENT APPROACH

Identify threats

Understand the external cyber security threats to the ship.

Understand the internal cyber security threat posed by inappropriate use and poor cyber security practices.

Identify vulnerabilities

Develop inventories of onboard systems with direct and indirect communications links.

Understand the consequences of a cyber security threat on these systems.

Understand the capabilities and limitations of existing protection measures.

Assess risk exposure

Determine the likelihood of vulnerabilities being exploited by external threats.

Determine the likelihood of vulnerabilities being exposed by inappropriate use.

Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.

Develop protection and detection measures

Reduce the likelihood of vulnerabilities being exploited through protection measures.

Reduce the potential impact of a vulnerability being exploited.

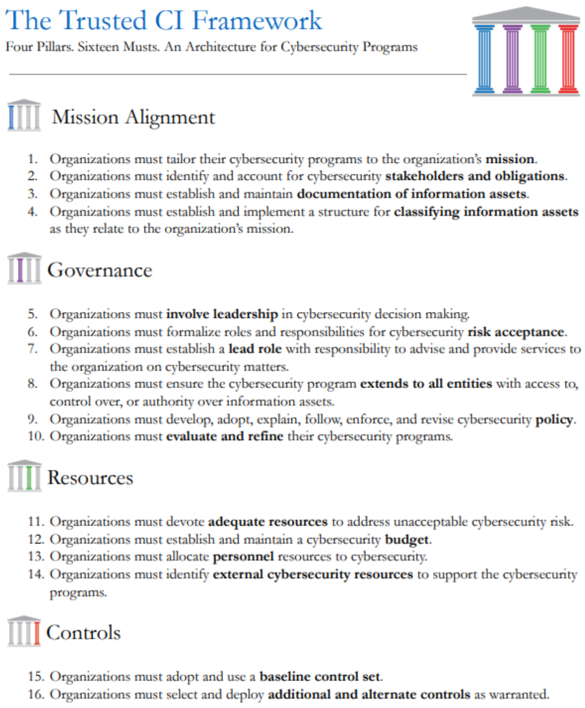
Establish response plans

Develop contingency plans to effectively respond to identified cyber risks.

Respond to and recover from cyber security incidents

Respond to and recover from cyber security incidents using the contingency plan.

Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.



The Trusted CI Framework

Four Pillars. Sixteen Musts. An Architecture for Cybersecurity Programs

Mission Alignment

1. Organizations must tailor their cybersecurity programs to the organization's **mission**.
2. Organizations must identify and account for cybersecurity **stakeholders and obligations**.
3. Organizations must establish and maintain **documentation of information assets**.
4. Organizations must establish and implement a structure for **classifying information assets** as they relate to the organization's mission.

Governance

5. Organizations must **involve leadership** in cybersecurity decision making.
6. Organizations must formalize roles and responsibilities for cybersecurity **risk acceptance**.
7. Organizations must establish a **lead role** with responsibility to advise and provide services to the organization on cybersecurity matters.
8. Organizations must ensure the cybersecurity program **extends to all entities** with access to, control over, or authority over information assets.
9. Organizations must develop, adopt, explain, follow, enforce, and revise cybersecurity **policy**.
10. Organizations must **evaluate and refine** their cybersecurity programs.

Resources

11. Organizations must devote **adequate resources** to address unacceptable cybersecurity risk.
12. Organizations must establish and maintain a cybersecurity **budget**.
13. Organizations must allocate **personnel** resources to cybersecurity.
14. Organizations must identify **external cybersecurity resources** to support the cybersecurity programs.

Controls

15. Organizations must adopt and use a **baseline control set**.
16. Organizations must select and deploy **additional and alternate controls** as warranted.

U.S. Academic Research Fleet
Cyberinfrastructure Working Group
ciwg@unols.org