OmniSOC

# Practical Cybersecurity Compliance for the US Academic Research Fleet

INMARTECH 2023
Will Drake

# Acronyms

- **ARF** - Academic Research Fleet
- **CRM** - Cyber Risk Management
- **CRMP** - Cyber Risk Management Plan
- **GCSOS** - Guidelines on Cybersecurity Onboard Ships
- **IMO** - International Maritime Organization
- **ISM** - International Safety Management
- **MSC** - IMO Maritime Safety Committee
- **NIST CSF** - National Institute for Standards and Technology Cyber Security Framework
- **SMS** - Safety Management System

# Presentation Outline

1. Introductions (Who are we?)
2. What is IMO CRM compliance?
3. ARF’s reasonable approach to compliance
4. Questions

# Introductions

# Introductions

- **US Academic Research Fleet** - 17 oceanographic vessels and various submersibles/autonomous vehicles owned by NSF, the Office of Naval Research (ONR), and U.S. universities and laboratories.

- **ResearchSOC/OmniSOC** - the shared cybersecurity operations center for higher education and research

# What is IMO Cyber Risk Management (CRM) Compliance?

# IMO CRM Compliance

- Combination of two amendments made to ISM Code:
  - **MSC.428(98)** - Maritime Cyber Risk Management in Safety Management Systems
  - **MSC-FAL.1/Circ.3** - Guidelines on Maritime Cyber Risk Management

# MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems

- Sets the requirement for cyber risk management to be incorporated into a ship’s Safety Management System (SMS)
- Sets deadline for appropriately addressing cyber risks – No later than first annual verification of Document of Compliance after 1/1/21.
- Points to MSC-FAL.1/Circ.3 for guidance on how to establish a maritime cyber risk management program.

# MSC-FAL.1/Circ.3 - Guidelines on Maritime Cyber Risk Management

- States that an effective CRM includes these functional elements:
  - Identify
  - Detect
  - Protect
  - Respond
  - Recover
- “For detailed guidance…users should refer to relevant international and industry standards and best practices.”

## Selecting a guideline

- Possible options include NIST CSF, ISO 27001, Guidelines for Cybersecurity Onboard Ships (GCSOS)
- ARF Security Team chose GCSOS because it is...
    - directly applicable to maritime environment without additional tailoring
    - Recognized by the IMO and US Coast Guard
    - Has a baseline control set built in

# A reasonable approach to compliance

# Considerations that should drive your compliance strategy

1. Leverage the language and intent of the requirements and guidance.
2. Within each control there is an easy win, or at minimum a path of least resistance. This should be your starting point to improve upon later.
3. The role of cybersecurity is to enable an organization’s mission.

# In their own words

- *Cyber risk management means the process of identifying, analysing, assessing and communicating a cyber-related risk and* ***accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders*** - IMO

- *One* ***accepted approach*** *to achieve the above is to comprehensively assess and* ***compare an organization's current, and desired, cyber risk management postures****. Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritized cyber risk management plan.*

# Approach

1. Formally adopt a guideline.
2. Document your CRM program and control implementation in a Cyber Risk Management Plan (CRMP), focusing on critical equipment.
3. While documenting control implementation identify and document programmatic and security gaps.
4. Use identified gaps and controls to perform a risk assessment.

# Approach

5. Create plans and timelines to mitigate identified risks.
6. Update the CRMP as systems and control implementations change.
7. Repeat steps 2-6 at least annually. Easiest way is to focus primarily on what has changed during that year.

# How the ARF Security Team helps

- We help ARF members by:
  - creating documentation templates
  - helping fill out CRMPs
  - providing guidance implementing security controls
  - performing gap/risk assessments and giving recommendations for mitigating risks
  - helping with audit/inspection preparation

# Questions?