# PREVIEWING CYBERSECURITY MANDATES

Jon C. Meyer, Information Systems Manager, SIO/UC San Diego

RVTEC, 21 Oct 2024

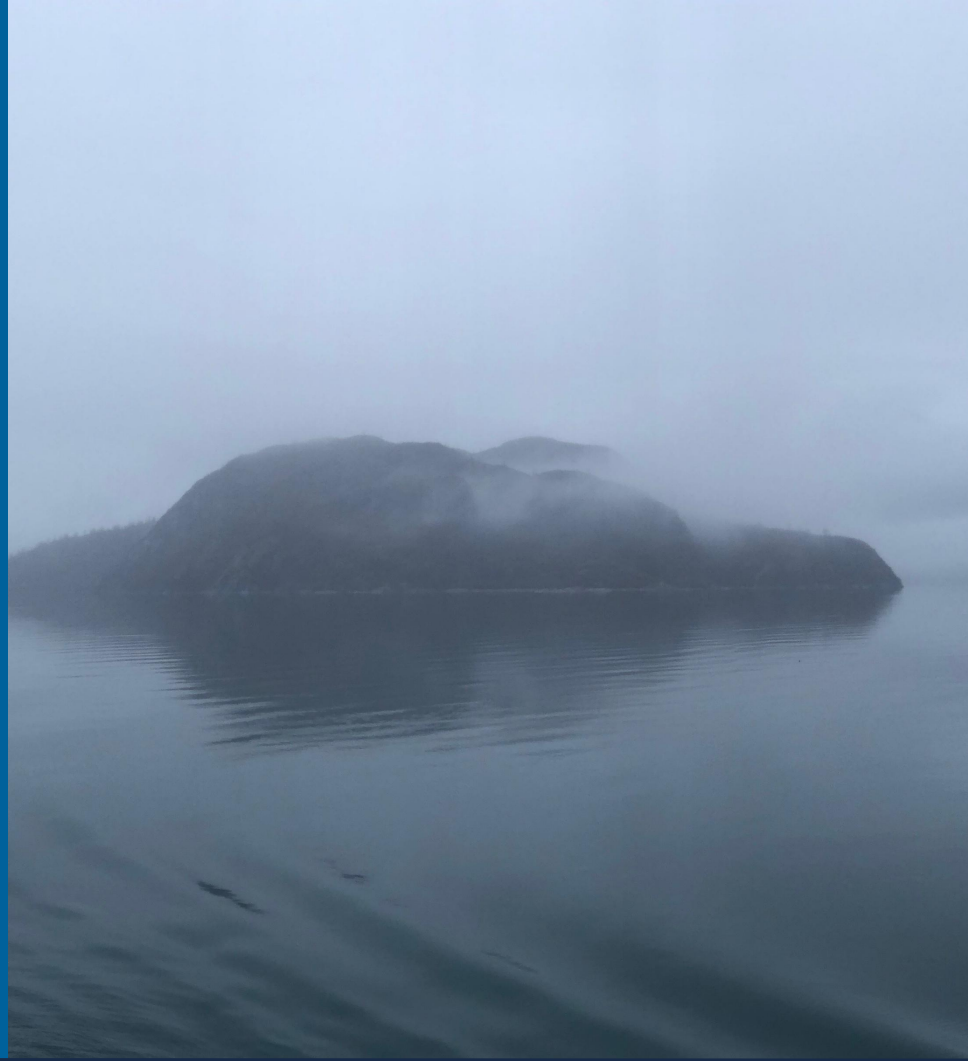
R/V *Sally Ride*, Anacortes , Washington. *Credit: Jeff Dillon.*

# About

- Worked at UC San Diego for 27 years, 18 at SIO
- Have supported aspects of remote/harsh environment support for a much of that time
- Passion for functional systems, at scale
- Research data at UC San Diego has a long history of being “open” and “free”
- Oversee HiSeasNet project (Internet), supporting ARF and USAP vessels
- Oversee the ScrippsIT unit (ShipCIS) which supports the CI aboard R/V Roger Revelle, R/V Sally Ride, R/V Robert Gordon Sproul and STARC Data Acquisition Systems aboard USCGC Healy

# Cybersecurity Mandates

- We will be exploring 3 systems affecting, or poised to affect aspects of research vessel operations:
  - UC San Diego Secure Connect (required)
  - SRG/STIGs (elective – somewhat)
  - A proposed rule, Cybersecurity in the Marine Transportation System (future)
- SIO is a somewhat unique position to be affected by all 3 systems because we run run a USCG-inspected marine facility, participate in the STARC project, and are part of the University of California system




# SECURE CONNECT

# *Secure Connect*

- Officially announced in Sep 2024
- UC San Diego's response to a  UC-wide directive about cybersecurity (1 of 9 UC campus' responses)
- Timeline of compliance: Q1 2025
- Ships have been explicitly discussed with our CISO and are considered "in scope"
- Is a joint effort of UC San Diego's IT Services, the Computer Security Operations Group (CSOG), departmental IT staff and Health Information Services, with oversight by the Cybersecurity Governance Committee and the Faculty Steering Committee.
- secureconnect.ucsd.edu for more details


## Introducing Secure Connect

Dear Technical Community,

Earlier this year, UC President Drake called on every UC location to meet a list of minimum security outcomes in order to strengthen the UC cybersecurity posture systemwide. These requirements, which are due to be in place by the end of May 2025, necessitate every member of the UC system to engage in cybersecurity efforts. The Secure Connect program is UC San Diego's response to this UC-wide call. The program is in alignment with the ongoing work at UC San Diego Health and other UC campuses.

The Secure Connect program will build upon our existing security measures to address compelling and critical security concerns in the constantly evolving cybersecurity landscape. We recognize that its implementation requires real and significant considerations regarding personal privacy, issues of

# *Secure Connect: Components*

- **Network Access Control (NAC):** Ensuring that only approved and secure devices can access our trusted networks (ucsd-protected, vpn, wired connections).
- **Vulnerability Management:** Requiring Qualys and Trellix on university-owned devices to proactively identify and mitigate security risks.
- **Endpoint registry (CMDB Integration):** Ensuring all university-owned assets and assets connected to our trusted networks are tracked within our Configuration Management Database.
- **Single Sign-On (SSO) Training Intercept:** Reminding users of upcoming training deadlines and redirecting them to training once the training is overdue, ensuring everyone is up-to-date with required cybersecurity awareness training.
- **Multi-Factor Authentication (MFA) on Email:** Ensuring multi-factor authentication for accessing email accounts to enhance protection against unauthorized access.
- **Enforcement of Minimum Security Standards for Personally Owned (BYOD) Devices:** Enforcing enabling of firewalls and requiring anti-virus software on BYOD devices connected to our trusted networks.
- ***NOTE:*** *UC San Diego Health has other requirements not listed, here*

# SECURE CONNECT, PREDICTED IMPACTS

- Most/all UC San Diego-owned endpoints are affected, or needs a documented exception in the CMDB
- More restrictive network segmentation will be needed – a mix of untrusted and trusted network segments
- BYOD networks on SIO ships will likely have to be treated as untrusted networks
- Data exchange networks (EG where cruise data can be accessed) will likely have to be considered a publicly accessible network of sorts
- SIO Researchers visiting other ARF vessels will have systems with Trellix HX, Qualys, etc on them, and will likely have to patch their OS and use 2FA VPN to maintain access to UC San Diego assets while underway.


SECURITY TECHNICAL
IMPLEMENTATION GUIDES (STIGS)

# *SRG/STIGs*

Security Technical Implementation Guides and Security Requirements Guides for the Department of Defense (DOD) information technology systems as mandated by DODI 8500.01.

This guidance bridges the gap between the National Institute of Standards and Technology Special Publication 800-53 and risk management framework (RMF)

Step-by-step instructions for many environments

Compliance with all tends to be less important than documenting the reason(s) you are not able to comply

Reviewed regularly (limited shelf life)

public.cyber.mil/stigs/ for more details


# *STIGs*

Pros:

- Easy to follow
- Very clear instructions for many systems
- Regularly maintained and up-to-date

Cons:

- More challenging to use some off-the-shelf systems
- Need people-time to maintain (quarterly is ideal)
- A fully “STIG’d” system may be so locked down that it is a challenge to get it to function
- elease dates

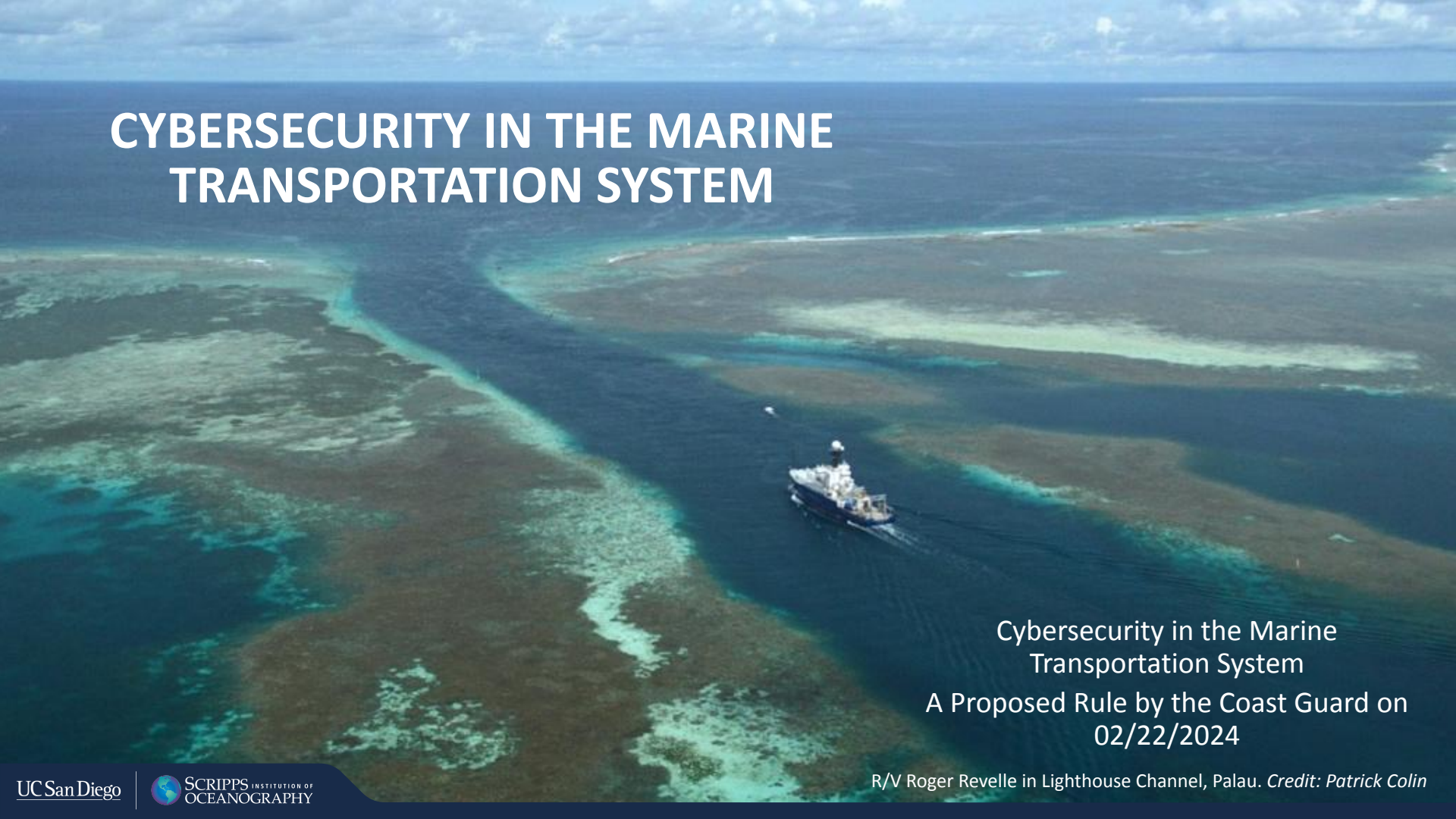
# PREDICTED IMPACTS, SRG/STIGS

- STIGs will be used by STARC to secure Data Acquisition Systems on USCG Healy to speak a common language with the vessel regarding how systems are secured
- Will required notable testing, since a system with full compliance
- Will likely influence how systems on SIO research vessels are secured as well
- Presumes some established infrastructure exists that some ships may not have, such as a Windows Domain Controller
- Could help define Mitigating Controls for

# CYBERSECURITY IN THE MARINE TRANSPORTATION SYSTEM

Cybersecurity in the Marine Transportation System

A Proposed Rule by the Coast Guard on 02/22/2024



R/V Roger Revelle in Lighthouse Channel, Palau. *Credit: Patrick Colin*

# Cybersecurity in the Marine Transportation System

Department of Homeland Security, Coast Guard, 33 CFR Parts 101 and 160, Docket No. USCG-2022-0802, RIN 1625-AC77

www.federalregister.gov/documents/2024/02/22/2024-03075/cybersecurity-in-the-marine-transportation-system

The Coast Guard proposes to update its maritime security regulations by adding regulations specifically focused on establishing minimum cybersecurity requirements for U.S.-flagged vessels, Outer Continental Shelf facilities, and U.S. facilities subject to the Maritime Transportation Security Act of 2002 regulations.

This proposed rule would help to address current and emerging cybersecurity threats in the marine transportation system. We seek your comments on this proposed rule and whether we should: use and define the term reportable cyber incident to limit cyber incidents that trigger reporting requirements, use alternative methods of reporting such incidents, and amend the definition of hazardous condition.

NATIONAL ARCHIVES

FEDERAL REGISTER

The Daily Journal of the United States Government

## Cybersecurity in the Marine Transportation System

A Proposed Rule by the Coast Guard on 02/22/2024

PUBLISHED DOCUMENT: 2024-03075 (89 FR 13404)

# Cybersecurity in the Marine Transportation System: excerpts

- *The maritime industry is relying increasingly on digital solutions for operational optimization, cost savings, safety improvements, and more sustainable business. However, these developments, to a large extent, rely on information technology (IT) systems and operational technology (OT) systems, which increases potential cyber vulnerabilities and risks. Cybersecurity risks result from vulnerabilities in secure and safe operation of vital systems, which increase the likelihood of cyber-attacks on U.S. facilities, OCS facilities, and U.S.-flagged vessels.*

- *Additional responsibilities of owners and operators of U.S.-flagged vessels, facilities, and OCS facilities would include:*

  - *Designating a CySO, in writing, by name and title, and identifying how the CySO can be contacted at any time. A CySO would have to be accessible to the Coast Guard 24 hours a day, 7 days a week*

  - *Ensuring that a Cybersecurity Assessment is conducted annually or sooner, under the circumstances described in this NPRM*

  - *Ensuring that a Cybersecurity Plan is developed and submitted for Coast Guard approval, either as a separate document or as an addition to an existing FSP, VSP, or OCS FSP*

  - *Operating the U.S.-flagged vessel, facility, or OCS facility in accordance with the approved Cybersecurity Plan; and*

  - *Reporting all cyber incidents, including TSIs, to the NRC and relevant authorities according to the Cybersecurity Plan.*

# PREDICTED IMPACTS, MARINE TRANSPORTATION SYSTEM


- We need to **wait** and see what edits USCG provides, following accepting public comments. Then, wait for the rule to take effect
- Inspected facilities and US-flagged vessels will need to designate a CySO
- Working with your host institution's CISO on what authority the CySO has is likely critical
- Start thinking about security drills for cyber
- Start thinking about security plans and how to digitally store them

# Summary

- There are many efforts afoot at the federal level, institutional level to secure systems
- Some specifically address maritime cyber-environments, some do not ,and operating vessels will need to consider how to adapt them
- These rules/frameworks/mandates are likely to affect workflows on research vessels for all persons
- Following some degree of cybersecurity mandate is more “when” than “if”
- OmniSOC supports ARF vessels in need!


THANK YOU. QUESTIONS?