

ARFSEC



Cybersecurity for the U.S Academic Research Fleet

Joint project of OmniSOC, a part of REN-ISAC, and the Center for Applied Cybersecurity Research (CACR) at Indiana University, funded by Cooperative Agreement with NSF

- **Previously a contract with OmniSOC, now a joint project of OmniSOC and CACR at Indiana University funded by a Cooperative Agreement with the NSF.**
- **Same staff, same mission:**
 - **Provide the fleet with a cybersecurity program and services to assist ship operators to maintain safe and reliable operations, meet regulatory requirements, and provide platforms to enable scientists to conduct research on the world's oceans, the Great Lakes and polar regions.**
- **Contact us:**
 - **Email - arfsec@iu.edu**

ARFSEC team



Mike Simpson
CISO



Ishan Abhinit



Mikeal Jones
Deputy CISO



Will Drake



Vishal Bhardvaj



ARFSEC Three Categories of Services:

1. Cybersecurity Operations & Technical Support
2. Cybersecurity Awareness & Organizational Resilience
3. Cybersecurity Governance, Risk, & Compliance



Cybersecurity Operations & Technical Support

Technical systems that enable cybersecurity operations across the fleet.

- Log and network monitoring, analysis and alerting, still using OmniSOC.
- Deploy and maintain network honeypots.
- General technical cybersecurity consulting to ship operators.
- Network vulnerability scanning and reporting.



Cybersecurity Awareness and Organizational Resilience

Strengthening fleet-wide cybersecurity culture and preparedness.

- Resources to prepare ship operators for Incident Response:
 - Developing policies and procedures.
 - Conducting tabletop exercises and cyber-incident drills.
- NSF Ship Inspections
- Community participation to share knowledge, support coordination, and gain insight into the cyberinfrastructure and threat landscape unique to fleet operations.
- Cybersecurity awareness training.



Cybersecurity Governance, Risk, and Compliance

Address cybersecurity risk and reduce the burden of navigating cybersecurity regulations and requirements.

- Supporting ship operators in:
 - Assessing risk
 - Identifying and implementing mitigation strategies
 - Documenting compliance
 - Preparing for inspections.
- Support both the advancement of cybersecurity in service of operational and research missions, and the fulfillment of obligations imposed by external regulations and the ship operators' parent institution.



Importance of cybersecurity



U.S. Coast Guard Cyber Command Maritime Cyber Alert

Information Sharing Protocol: **TLP:CLEAR** (<https://www.us-cert.gov/tlp>)

April 29, 2026

INC Ransom

■ Summary

Coast Guard Cyber Command (CGCYBER) is drawing attention to the threat posed by the INC Ransom group, which has demonstrated the capability to target the U.S. Marine Transportation System (MTS) using sophisticated tactics, techniques, and procedures (TTPs). This threat actor gains initial access by exploiting unpatched public-facing applications and through targeted phishing campaigns. Once a foothold is established, the threat actor moves laterally using legitimate network administration tools, attempting to escalate privileges and disable security controls. Ultimately, INC Ransom appears to be a financially motivated group that employs a 'double extortion' model, exfiltrating sensitive data prior to encryption and demanding payment for both data decryption and the non-disclosure of stolen information.



Importance of cybersecurity



U.S.
Ma



US government warns of severe CopyFail bug affecting major versions of Linux

Zack Whittaker 3:21 PM PDT · May 4, 2026

Summary

Coast Guard
which has d
sophisticate
unpatched
established
escalate pri
motivated g
demanding

IMAGE CREDITS: [LUKAS / UNSPLASH](#)

Importance of cybersecurity



E

4 ALBERT EMBANKMENT
LONDON SE1 7SR

Telephone: +44 (0)20 7735 7611

Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3/Rev.3
4 April 2025

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT



Importance of cybersecurity



UNITED STATES COAST GUARD NEWS
DEPARTMENT OF HOMELAND SECURITY

NEWS HOME ▾

NEWS BY REGION ▾

PACIFIC AREA

ATLANTIC AREA

JOIN THE COAST GUARD

OUR ORGA

Final Rule: Cybersecurity in the Marine Transportation System

Jan. 17, 2025

The Coast Guard has published a [final rule in the Federal Register](#) to update cybersecurity requirements for U.S.-flagged vessels, Outer Continental Shelf (OCS) facilities, and facilities subject to Maritime Transportation Security Act of 2002 (MTSA).



Importance of cybersecurity



UNITED STATES COAST GUARD NEWS

DEPARTMENT OF HOMELAND SECURITY

NEWS HOME

Fire

PRESIDENTIAL MEMORANDA

Presidential Memorandum on United States Government- Supported Research and Development National Security Policy

— NATIONAL SECURITY & DEFENSE | Issued on: January 14, 2021



Importance of cybersecurity



UNITED STATES COAST GUARD NEWS

DEPARTMENT OF HOMELAND SECURITY

NEWS HOME

FIR

De

PRESIDENTIAL MEMORANDA

Presidential Memorandum on United States Government

119TH CONGRESS
1ST SESSION

H. R. 1223

IN THE SENATE OF THE UNITED STATES

MAY 21, 2025

Received; read twice and referred to the Committee on Commerce, Science, and Transportation

AN ACT

To require a plan to improve the cybersecurity and telecommunications of the U.S. Academic Research Fleet, and for other purposes.

Acknowledgements

*ARFSEC is supported by the National Science
Foundation under Award No. 2602167*

