Funded by the National Science Foundation, Grant #2127548

Lee Ellett: Academic Research Fleet Cyberinfrastructure Working Group

Lightning Talks

March 1, 2022
CI Compass Cyberinfrastructure for NSF Major Facilities Workshop

USC Viterbi School of Engineering Information Sciences Institute
INDIANA UNIVERSITY
UNIVERSITY OF NOTRE DAME
THE UNIVERSITY OF UTAH
TEXAS TECH UNIVERSITY
renci

Lightning Talk
Academic Research Fleet
Cyberinfrastructure Working Group

Lee Ellett

Academic Research Fleet (ARF)

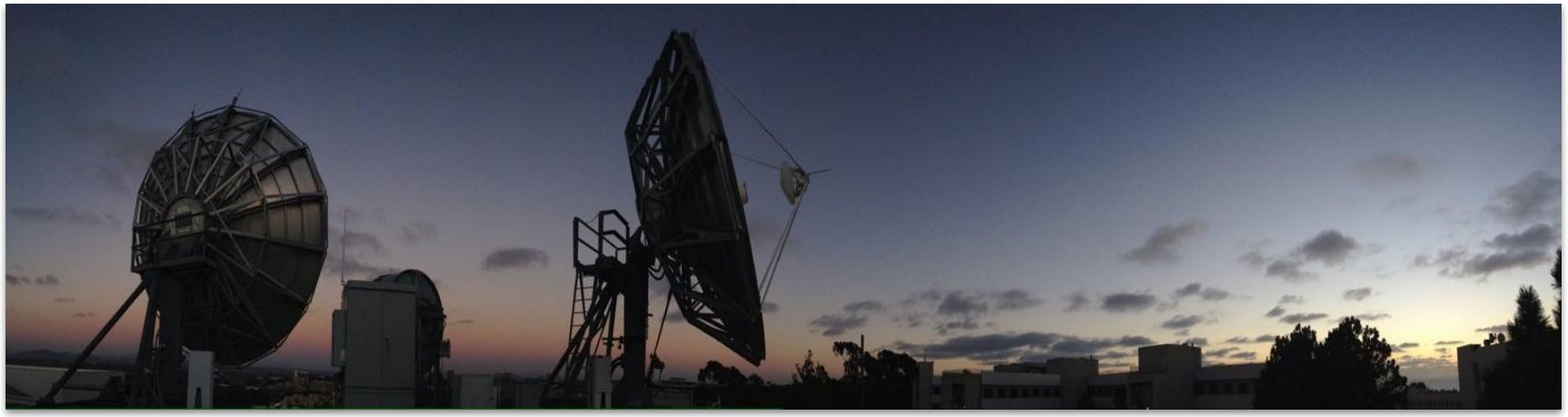
- 14 Vessel Operating Institutions
- 18 Research Vessels
- University National Oceanographic Laboratory System (UNOLS) – Coordinating Organization

Why was ARF CIWG established?

- Modern Research Vessels have been delivered with more operational technology and greater reliance on cyberinfrastructure
- Cybersecurity requirements coming into effect have been increasing the complexity of the operational environments on vessels
- The group was initially established to review the Trusted CI engagement report and provide guidance on priorities and efficient approaches to our federal sponsors

Unique Cyberinfrastructure Challenges

- Operational Technology – Engine Control Systems, Winch Systems, Integrated Bridge Systems
- Limited bandwidth available for vessels at sea using geostationary satellite communications



Working Group Participants

John Haverlack - UAF
Laura Stolp - WHOI
Ken Feldman – UW
Robert Kamphaus - UW
Pam Clark – WHOI
Jon Meyer – SIO
Lee Ellett – SIO
Chris Romsos – OSU
Jules Hummon – UH
Scott Ferguson – UH
Erich Grubel – URI
Brandi Murphy – UNOLS Office

Regulatory Environment

Agencies and Frameworks

1. International Maritime Organization (IMO)
   a) Requires the addition of a Cyber Risk Management Plan (CRMP) for inspected vessels
2. Department of Defense (DoD)
   a) Defense Acquisition Regulation Supplement (DFARS)
   b) Cybersecurity Maturity Model Certification (CMMC)
3. United States Coast Guard (USCG)
   a) Strategic Cyber Outlook
   b) Published Cyber Threats
4. National Science Foundation (NSF)
   a) Cybersecurity and Cyberinfrastructure Plan requirements in Major Facilities Guide

2021 Cybersecurity Pilot Program (UH, UW, WHOI)

The National Science Foundation (NSF) supported a Pilot Program that has been successful, where all vessels passed their first inspections with a Cybersecurity Risk Management Plan (CRMP) as a requirement. These will require continual improvement.

Through the process of the Cybersecurity Pilot Program and guidance from the Cyberinfrastructure Working Group (CIWG) it was confirmed that the operation of ONR vessels with few exceptions do not have Controlled Unclassified Information (CUI) DFARS 252.204-7012. CIWG agrees that CMMC level 1 is the best baseline moving forward.

NSF supports the continued need for a Cybersecurity Program to address the needs of the 18+ ships of the US Academic Research Fleet (ARF) in order to maintain the IMO Cybersecurity requirements.

2022 ResearchSOC Year 1

Statement of Work Highlights

1. ResearchSOC – OmniSOC 24/7 monitoring and alerting
2. Vulnerability Identification Service
3. Virtual Chief Information Security Officer (vCISO)
4. Virtual Security Team
5. Red Phone IR Service

The scope of ResearchSOC services for 1 year are targeted at accelerating the establishment of a Cybersecurity program for the ARF.