ARF Cyberinfrastructure Updates

UNOLS May 2023
Presentation Overview

**Satellite Communications**
- SatComm Internet Updates

**Cyberinfrastructure**
- Fortigate NextGen Firewall Upgrades

**Cybersecurity**
- ResearchSOC / OmniSOC Updates
ARF CI Committees

- **SatNAG** - Satellite Network Advisory Group
- **CIWG** - Cyberinfrastructure Working Group
  - Operations Focus
  - Science Focus
- **HiSeasNet**
- **NextGen Firewall**
Satellite Communications

20/20 Bandwidth Expansions
- Expansion on SeaLink VSAT
- On ONR Vessles + Sikuliaq
- Thru 2024
- Nominal Bandwidth 4/2 Mbps
- Expansion BW is 20/20 Mbps
  - LTE Cellular Equiv
- Significant impact to productivity and moral

StarLink
- Managed by HSN
- LEO
- StarLink Maritime service now available
  - ~ 100 / 6 Mbps
- Supply chain delays
- Installed on Revelle
- ~ Worldwide coverage

Iridium Certus
- Managed by HSN
- LEO
- 5 GB per month per vessel
- 5 vessel participating

Day Rate Changes
- $atComm expenses are no longer part of vessel day rates
Next Gen Firewall
- Opt-In Service for ARF Vessels
- Engagement by multiple ARF institutions
- Supports both Operations and Science
- Fortigate Firewall have been selected
- Test bed system being developed at URI
- Hardware Procurement in late 2023 by UCSD

Provides
- Seamless Internet access over Multiple SatComms
- Better Security Reporting for Cybersecurity Audits and Compliance
Cybersecurity

ARF Cybersecurity Program
Contracted with ResearchSOC and OmniSOC to provide fleetwide protocols and resources including:
- Chief Information Security Officer (CISO) - Ryan Kiser, IU
- Cyber Risk Management Templates
- Vulnerability Scanning
- Security Information and Event Management
- Incident Response
- Bi-weekly meetings
- Supporting Operations and Science services

Inspections
- 1 facility NCAR
- Most vessels are passing inspections
- Will be part of NSF inspections
- CMMC compliance is coming from the Institution side.

Risks
- Ability to Respond Quickly
Additional Reference Slides
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.
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.

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.

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.


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

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

Cyberinfrastructure Working Group

ciwg@unols.org

RVTEC 2022-11-01
IT Security Zones
(~Tech Services)
- Transient Systems (WiFi)
  - Science Party
  - Crew
  - Contractors
- Shared CI
  - DNS
  - File Shares
  - Web
  - Printers

OT Security Zones
(~Operations)
- Operational Technology
  - Crew Kiosks
- Isolated (AirGap) Networks
  - Eng
  - Bridge
  - CCTV

Science / DAS
- Data Storage
- Instrumentation

https://zenodo.org/record/6828675
Partnerships

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