NSF Trusted CI Engagement Update

Lee Ellett

What is Cyberinfrastructure?

Cyberinfrastructure (CI):

"consists of computing systems, data storage systems, advanced instruments and data repositories, visualization environments, and people, all linked together by software and high-performance networks to improve research productivity and enable breakthroughs not otherwise possible."

Credit: Craig A. Stewart, et al. 2010."What is cyberinfrastructure" SIGUCCS'10.ACM, New http://doi.acm.org/10.1145/1878335.1878347

Examples of Cyberinfrastructure within the ARF

Vessels

Instrumentation Computers
Instrumentation Information Systems
Workstation Systems
Engine Control Systems
Integrated Bridge Systems
Winch Control Systems
Telemedicine Systems
Winch Information Systems
Servers (email, file, etc)
Network Firewall Appliances
Wired Network
Wireless Network
Voice and Video Systems

Fleet Activities

Ship Time Request System
HiSeasNet
Secondary Satellite Network
R2R
SAMOS
UHDAS
Multibeam Advisory Committee
Oceanographic Data Facility (ODF)
MISO - PFPE

Legend:

Blue = Oceanographic Technical Services
Red = Ship Operations
Green = Mutually Critical

What is Cybersecurity?

Cybersecurity:

the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

Information Security:

the state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this.

Examples of Relevant Cybersecurity Requirements

1. IMO Maritime Cyber Risk Management in Safety Management Systems
2. Defense Federal Acquisition Regulation Supplement 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
3. NSF Major Facilities Manual (Sept 2019)

NSF Trusted CI Mission Statement

The mission of Trusted CI is to lead in the development of an NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leader in research and innovation.

This mission is accomplished through one-on-one engagements with projects to address their specific challenges; education, outreach, and training to raise the state of security practice across the scientific enterprise; and leadership on bringing the best and most relevant cybersecurity research to bear on the NSF cyberinfrastructure research community.

This is an NSF-funded effort to bring relevant cybersecurity to research projects

NSF Trusted CI Team for ARF Engagement

Mark Krenz

Chief Security Analyst, IU Center for Applied Cybersecurity Research

Ryan Kiser

Senior Security Analyst, IU Center for Applied Cybersecurity Research

Ishan Abhinit

Senior Security Analyst, IU Center for Applied Cybersecurity Research

Andrew Adams

Senior Information Security Analyst, Pittsburgh Supercomputing Center

John Zage

Research Programmer, National Center for Supercomputing Applications

Kelli Shute

Project Manager, IU Center for Applied Cybersecurity Research

ARF Team For NSF Trusted CI Engagement

John Haverlack

University of Alaska, Fairbanks – Acting CISO for Engagement

Brandi Murphy

UNOLS Office

Jon Meyer

Scripps Institution of Oceanography

Lee Ellett

Scripps Institution of Oceanography

ARF Engagement Plan

1. For Trusted CI to review available policies, procedures, and documentation pertaining to the security of ARF as an organization and to the ships organized through UNOLS.

2. For Trusted CI to write and deliver a report to the ARF providing recommendations for how ARF's cybersecurity policies and procedures can be improved to reduce cybersecurity risks to the organization and to science and research projects utilizing their vessels and services.

Continued…

ARF Engagement Plan

3. To identify problems with the existing state of CI, practices, and requirements and develop a set of improvements which are practical for the ARF to implement.

- Determine an optimal organizational and resourcing structure to better equip the fleet to handle the evolving CI and cybersecurity demands of fleet constituents.
- Develop a common set of security practices which can be implemented across the fleet to allow ships both to adhere to cybersecurity requirements such as IMO 2021 and to adequately secure the growing body of operational cyberinfrastructure onboard.

Summary of Trusted CI Engagement Timeline

July 2, 2019: Regular weekly meetings commence, begin drafting blog post announcing engagement.
July 19, 2019: Engagement plan final draft complete, final review begins
July 24, 2019 (MILESTONE): Engagement plan signoff target date, formal engagement effort begins.
Dec 17, 2019 (MILESTONE): Target date for completion of all deliverables.
Jan 7, 2020 (MILESTONE): Formal end of engagement activities. All written deliverables delivered to and accepted by US Academic Research Fleet by this date.

Uncommon Security Challenges Observed

- It’s a vehicle!
- Very short and infrequent maintenance windows
- Very low bandwidth while at sea
- Low budget for security mandates
- High crew turnover
- Science parties' BYODs
- IoT everywhere
- Unique hardware
- Potentially life risking situations
- Travel to foreign ports
- Remote only access only for security checks
- Unusual console locations, sharing
- Policies that aren’t compatible with institutional security controls
- Limited Space/Overlapping purposes of rooms

*Courtesy Mark Krenz Trusted CI Presentation to RVTEC Oct 2019

Governance Observations

- As a Large Facility, the ARF does not have a central structure that defines an accountability framework for Cybersecurity
- The NSF Major Facilities Guide requires that NSF Large Facilities have a Cyberinfrastructure Plan and a Cybersecurity Plan
- "A cybersecurity program should be scoped to the key assets, resources, and the full lifespan of the facility. It is necessarily a living program that adapts, adjusts, and advances."
- Similarities exist to the approach taken for other legal requirements addressed in the RVSS

Roles and Responsibilities

Cyberinfrastructure has become critical to safe and efficient research vessel operations and is also critical to conduct transformative scientific research. Roles and responsibilities for the operation and maintenance of this critical infrastructure are not clearly defined in our program.

<u>Individual Programs within NSF Solicitation 19-602</u>

1. Ship Operations (Ship Ops)
2. Oceanographic Technical Services (Tech Services)
3. Oceanographic Instrumentation (OI)
4. Shipboard Scientific Support Equipment (SSSE)
5. Ship Acquisition and Upgrade (SAU)
6. Other Facility Activities (OFA)

Ship Operations

The NSF Ship Operations Program provides support for costs associated with the operation and maintenance of vessels in the U.S. Academic Research Fleet (ARF). Allowable costs include salaries and related expenses of crew members and marine operations staff; acquisition of minor or expendable equipment; maintenance, overhaul and repairs; insurance; and direct operating costs such as fuel, food, supplies, travel, and pilot and agent fees. Shore-side facilities and support costs are provided only to the extent that they relate directly to ship operations. Ship Operations support requests must be directly attributable to NSF-sponsored science.

Key Point: The RCRV Program has called for an Electro Technical Officer in their crewing plan. There are other examples on non-UNOLS use of this position on research vessels.

Oceanographic Technical Services

The Tech Services Program provides support of institutional technical services to enhance the scientific productivity of research programs using major facilities, primarily research vessels. Research vessel technical services include quality assurance, scheduling of technical support, logistical assistance, and at-sea supervision of the instrumentation and shared-use equipment available to sea-going researchers. This program also provides baseline operational support for the University-National Oceanographic Laboratory System (UNOLS) equipment pools (wire, vans and winches). Support of research vessel technical services and UNOLS equipment pools includes salaries and related expenses, maintenance and calibration of sensors and instrumentation, and associated travel.

Key Point: Tech Services responsibilities have expanded beyond instrumentation to support the majority of vessel CI. Expertise in CI is generally a different skillset than what is expected for research instrumentation support.

Oceanographic Instrumentation

The OI Program provides support to enhance the scientific capabilities and productivity of seagoing research projects that use major facilities, primarily research vessels. Proposals may include shared-use instrumentation for the collection, processing and analysis of oceanographic data. Typical instrumentation includes sensors, acoustic systems, data loggers, water sampling rosettes, biological net systems, coring equipment and auto-analyzers. Proposals must be for instrumentation that will support multiple research projects.

Key Point: This is where the majority of vessel CI hardware requests are proposed. This does place CI hardware in direct competition with instrumentation funds.

Shipboard Scientific Support Equipment

The SSSE Program provides support to improve safety and enhance scientific capabilities and productivity of seagoing research programs that use major facilities, primarily research vessels. Proposals may include new permanent or portable equipment required to outfit a vessel to conduct oceanographic research as well as overhaul of equipment previously funded under this program including science handling systems (winches, frames, cranes, etc.), navigation and communication equipment, and safety and regulatory-related items. Requests for purchase of new winch pool or van pool capital equipment must be submitted to this program. SSSE proposals are generally submitted by the institution's Marine Superintendent whose operational funding is provided through the Ship Operations Program in Ocean Sciences.

Continued…

Shipboard Scientific Support Equipment (cont'd)

There are enough differences in organizational structure throughout the fleet to make combining the SSSE and OI programs problematic. In addition, the average cost for SSSE requests are orders of magnitude more than average OI requests. In the interest of having similar size proposals competing against each other, the SSSE and OI programs will remain separate.

Key Point: The rationale for having separate SSSE and OI programs could also be applied to CI hardware.

In Summary

- The Trusted CI report will be delivered Jan 2020 and be used to make recommendations to UNOLS Council on Cybersecurity
- Trusted CI has noted unique challenges with the ARF due to the sea going aspect and due to the distributed nature
- The ARF should consider a Cyberinfrastructure Plan as outlined in the Major Facilities Manual
- In parallel, we are providing information to the NSF funded Cyberinfrastructure Center of Excellence Pilot Program (presentation to follow) to gain awareness of best practices across NSF Large Facilities