Report on NSF Large Facility Cyberinfrastructure Activities

Introduction of NSF Trusted CI Engagement

Lee Ellett

What is Cyberinfrastructure?

Cyberinfrastructure "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

2017 Workshop on Cyberinfrastructure for Large Facilities

Workshop Key Recommendations (Full Report at facilitiesci.org)

- Foster the creation of a facilities' CI community and establish mechanisms and **resources to enable the community to interact, collaborate, and share**.
- Support the creation of a curated portal and knowledge base to enable the discovery and sharing of **CI-related challenges, technical solutions, innovations, best practices, personnel needs, etc., across facilities** and beyond.
- **Establish a center of excellence** (following a model similar to the NSF-funded Center for Trustworthy Scientific Cyberinfrastructure, CTSC) as a resource providing expertise in CI technologies and best practices related to large-scale facilities as they conceptualize, start up, and operate.
- **Establish structures and resources** that bridge the facilities and that can strategically address workforce development, training, retention, career paths, and diversity, as well as the overall career paths for CI-related personnel.

Cyberinfrastructure Center of Excellence Pilot Program

CI CoE Pilot Project Goals

- Dedicated to the enhancement of CI for science
- Platform for knowledge sharing and community building
- Key partner for the establishment and improvement of Large Facilities with advanced CI architecture designs
- Grounded in re-use of dependable CI tools and solutions
- Forum for discussions about CI sustainability and workforce development and training
- Pilot a study for a CI CoE through close engagement with NEON and further engagement with other LFs and large CI projects.

Connecting the ARF with CI CoE Pilot

2019 NSF Workshop Connecting Large Facilities and Cyberinfrastructure – Sept 2019

Participation in CICoE Working Groups

- Data Life Cycle and Disaster Recovery
- Identity Management

2019 Fall Council Meeting

- CI CoE Presentation to UNOLS Council

Background on NSF Trusted CI Engagement

Cybersecurity topics at 2018 RVTEC Managers Meeting

- Upcoming 2021 IMO Cybersecurity requirements
- Design and management of increasing complex shipboard networks
- Management of shipboard firewall appliances
- Basic Services has evolved to include IT support for crew and science, this is impacting instrumentation support
- Increase in support of operational technology on modern vessels

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.

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 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.

ARF Trusted CI 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.