Cyber Infrastructure / Cyber Security
UNOLS Annual Meeting 21 October 2020

What is Cyberinfrastructure

Cyberinfrastructure includes all **physical and digital assets** used in providing information technology services for the communication, storage and processing of digital information.

Physical assets include computers, servers, networking equipment, data centers, and even commodity components like keyboards, flash drives, etc.

Digital assets are less tangible and would include software, data sets, databases, radio spectrum, capacity planning, AC power, HVAC (cooling), and network bandwidth and connectivity.

A cyberinfrastructure plan addresses cradle to grave lifecycle and maintenance issues to keep aging physical and digitals assets up to date, at adequate capacity for the mission, and monitored for health and security. This is necessary to be proactive before there are issues, as opposed to being reactive after a data loss or service loss event has already happened.

What is Cybersecurity

A very broad term but is based on three fundamental concepts known as " The CIA Triad ": **Confidentiality, Integrity and Availability**. It is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. An important component of the larger **Cyberinfrastructure Plan.**

Cybersecurity address who has what level of access to which assets. This is called **authentication**, which commonly includes proof of something only that person knows, like a password. Multi-factor authentication, which is becoming more common, can require proof of something a person knows, coupled with something they have, like a key. Once sufficiently authenticated the identified person can access assets for which they are authorized. **Authorization** can be given at different levels to different assets to different people. Some persons may only be given read-only access to view a document while other persons may be granted read-write access to modify or delete a document.

The Law

- Each Operator will need to develop and integrate a Cybersecurity Risk Management (CRM) Plan into their Safety Management System (SMS) by the time of their first external ABS Document of Compliance (DoC) Survey in 2021.

- NSF Large Facilities Guide (ARF vessels are considered a large facility) requires the establishment of a robust Cybersecurity plan.

Who is responsible ?

- Ship Operations/Superintendents/port captains?

- The technicians?

- Need a single point of contact at each institution.

What are we doing

- Trusted CI Engagement happened across the fleet. Recommendations were written and a link is available for Lee Ellett's review of the recommendations for the fleet at the spring meeting.
- Pilot Program initiated to bring ships into IMO compliance during 2021.
- A Cybersecurity working group has been established comprised of techs and operations personnel to discuss Cybersecurity in the ARF and advise NSF regarding the path forward.

Where are we going/thinking?

The Cybersecurity working group is writing Terms of Reference for acceptance as an official UNOLS Committee. This will be presented at the next Council Meeting for discussion/approval. Topics that the working group is focusing on include:

- Should a Cybersecurity plan be integrated into the Research Vessel Safety Standards (RVSS) ?
- As was recommended by Trusted CI, does the fleet need to have a Chief Information Security Officer (CISO) and/or a Chief Information Technology Officer (CITO) ?
- Is the current solicitation for NSF proposals (NSF19-602) adequate or should it be re-written to define which program (Ship Ops, Tech Services) has responsibility for cyberinfrastructure/Cybersecurity?
- Is the time right to create another program within NSF IPS to deal specifically with the fleet's Cyberinfrastructure?