UC San Diego

CYBERSECURITY AND CYBERINFRASTRUCTURE ACTIVITIES AT SIO AND INTRODUCTION OF PEREGRINE TECHNICAL SOLUTIONS
04/24/2019

Lee Ellett, SIO, Manager Shipboard Technical Support

UC San Diego

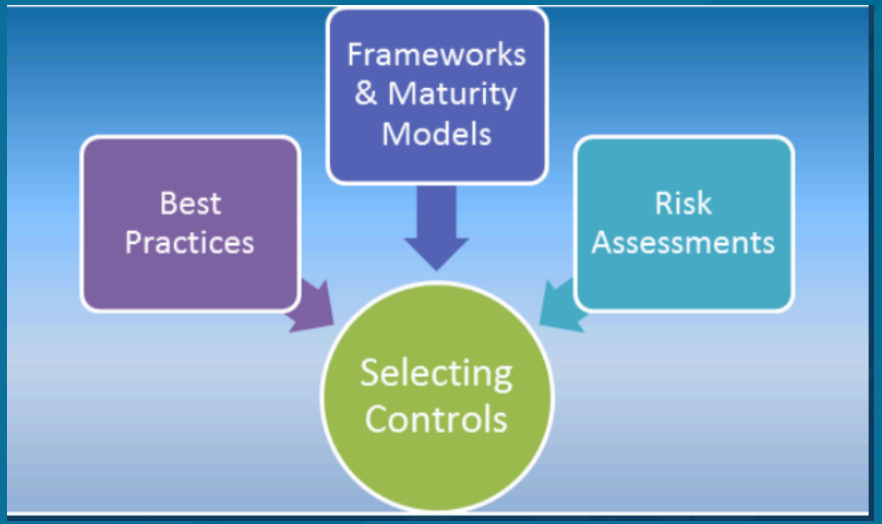
CYBERSECURITY

What is a Cybersecurity Program

"A cybersecurity program is a structured approach to develop, implement, and maintain an organizational environment conducive to appropriate information security levels of information-related risk. Cybersecurity programs entail ongoing activities to address relevant policies and procedures; technology and mitigations; and training and awareness. Cybersecurity programs are scoped to key assets, resources, and lifespan of organizations" - CTSC

Credit: Center for Trustworthy Scientific Cyber infrastructure (CTSC) Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects

Cybersecurity Regulatory Frameworks, Standards, and Programs



Credit: Center for Trustworthy Scientific Cyberinfrastructure (CTSC) Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects

- International Maritime Organization (IMO) Cybersecurity Guidelines
- NSF Trusted CI Program
- National Institute of Standards and Technology (NIST) Cybersecurity Framework and Standards
- Defense Federal Acquisition Regulation Supplement (DFARS) 252.204.7012
- International Organization for Standardization (ISO) 27001

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

***

IMO Guidelines for Cyber Risk Management

- Will apply to inspected Vessels after 1 JAN 2021
- Based on NIST Cybersecurity Framework
- Based on ISO 27001

EVALUATION OF CYBERSECURITY STANDARDS AND REGULATIONS

- UCSD Information Technology Services, SIO Scripps IT, and UCSD export control were engaged to discuss campus security plans and future policies that are being implemented

- Jan 2019, SOMTS hosted a two day site visit by Peregrine Technical Solutions LLC. resulting in a quotation for developing an IMO process and vessel assessments

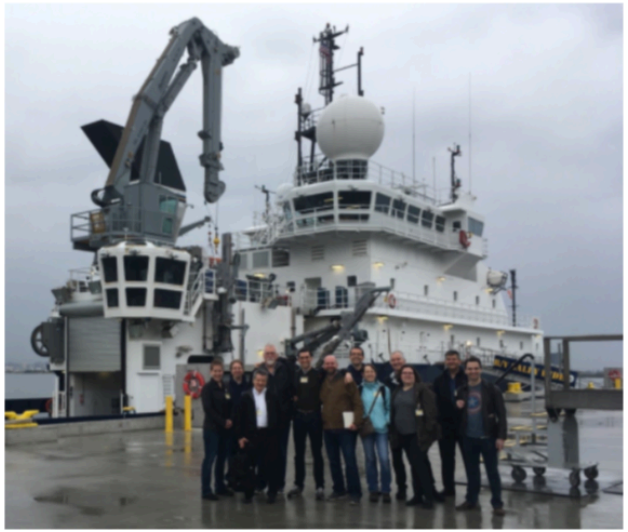
- Based on all the input we have received the most likely direction is that academic institutions receiving ONR funds will need to implement the cybersecurity controls that are compliant with DFARS 7012/NIST 800-171

Wednesday, March 20, 2019

Scripps Institution of Oceanography, Trusted CI, and CACR Launch Engagement

We are pleased to announce the start of an engagement with Scripps Institution of Oceanography at the University of California San Diego. Scripps Oceanography is supported by multiple NSF awards, including # 1327683, 1212770, and 1556466, as well as research awards from the Department of Defense and National Oceanographic and Atmospheric Administration (among others).

This engagement is in collaboration with the DOD-funded Principles-Based Assessment for Cybersecurity Toolkit (PACT) project. PACT is a methodology and tool set based on the Information Security Practice Principles and developed in collaboration by Trusted CI, the IU Center for Applied Cybersecurity Research, and Naval Surface Warfare Center Crane. Lessons learned from applying the methodology to Scripps Oceanography will be used to refine PACT. Scripps Oceanography's interest in engaging with Trusted CI and the PACT project presented a perfect opportunity to leverage Trusted CI's expertise and knowledge of complex open science environments, while advancing a methodology with potential for very broad application.



NSF Trusted CI Program

- Trusted CI's mission is to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.
- During the DOD-funded PACT project site visit STS was encouraged to apply for a 2019 NSF trusted CI engagement
- On 04/03/19 an application for an engagement was submitted. SIO, UAF, UH, OSU, UW, LUMCON, and WHOI to represent a broad cross section of the US ARF

UC San Diego

CYBERINFRASTRUCTURE

What Is Cyberinfrastructure

Cyberinfrastructure(CI): Research environments that support advanced data acquisition, data storage, data management, data integration, data mining, data visualization and other computing and information processing services distributed over the Internet beyond the scope of a single institution.

Credit: Center for Trustworthy Scientific Cyber infrastructure (CTSC) Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects

Use of Computing Clusters on SIO Vessels and STS Projects

Since late 2016 STS has been purchasing and deploying high availability computing clusters in support of department projects to replace aging cyberinfrastructure.

- Shore Datacenter
- R/V *Roger Revelle*
- R/V *Sally Ride*
- R/V *R.G. Sproul*
- USCGC *Healy* (STARC)

SATELLITE COMMUNICATIONS INFRASTRUCTURE IN THE US ARF

HiSeasNet-enabled vessels, with year of hardware commissioning and antenna brand/model. More than half include hardware beyond the antenna service life of nine years.

Global Class Ships	**Year**	**Antenna**
R/V *Thomas G. Thompson*	2018	Sea Tel 9711 IMA, C-band/Ku-band
R/V *Roger Revelle*	2007	Sea Tel 9797B
R/V *Atlantis*	2003	Sea Tel 9797A-B, C-band
R/V *Sikuliaq*	2012	Sea Tel 9711 IMA, C-band/Ku-band
R/V *Marcus Langseth*	2007	Sea Tel 9797B
Ocean/Intermediate Class Ships		
R/V *Kilo Moana*	2006	Sea Tel 9797A-B, C-band
R/V *Oceanus*	2007	Sea Tel 6006, Ku-band
R/V *Endeavor*	2012	Sea Tel 6012, Ku-band
R/V *Atlantic Explorer*	2009	Sea Tel 6006, Ku-band
R/V *Neil Armstrong*	2016	Sea Tel 9711 IMA, C-band/Ku-band
R/V *Sally Ride*	2017	Sea Tel 9711 IMA, C-band/Ku-band
Coastal/Local Class Ships		
R/V *F.G. Walton Smith*	2007	Sea Tel 6006, Ku-band

CYBERSECURITY AND CYBERINFRASTRUCTURE WORKING GROUP

- Form a Cybersecurity and Cyberinfrastructure Working Group to develop a white paper with recommendations for UNOLS Council endorsement
  - 2 RVOC positions
  - 2 RVTEC positions
  - 2 Scientist, Ship Users
  - UNOLS SatNAG
- Cybersecurity subject matter expertise should also be included
- Clearly defining cybersecurity and cyberinfrastructure needs for the US ARF will strengthen the requests for resources to the federal agencies
- These are challenges that other Large Facilities have faced; this coordination is a recommended next step for the US ARF