Cyberinfrastructure Working Group
UNOLS Annual Meeting
25 October 2021

Working Group Participants

John Haverlack - UAF
Laura Stolp - WHOI
Ken Feldman – UW
Robert Kamphaus - UW
Pam Clark – WHOI
Jon Meyer – SIO
Lee Ellett – SIO
Chris Romsos – OSU
Jules Hummon – UH
Scott Ferguson – UH
Erich Grubel – URI
Brandi Murphy – UNOLS Office

Cybersecurity

Agencies and Frameworks

1. International Maritime Organization (IMO)
    a) Requires the addition of a Cyber Risk Management Plan (CRMP) for inspected vessels
2. Department of Defense (DoD)
    a) Defense Acquisition Regulation Supplement (DFARS)
    b) Cybersecurity Maturity Model Certification (CMMC)
3. United States Coast Guard (USCG)
    a) Strategic Cyber Outlook
    b) Published Cyber Threats
4. National Science Foundation (NSF)
    a) Cybersecurity requirements in Major Facilities Guide

Pilot Program Background

The National Science Foundation (NSF) supported a Pilot Program that has been successful, where all vessels passed their first inspections with a Cybersecurity Risk Management Plan (CRMP) as a requirement. These will require continual improvement.

Through the process of the Cybersecurity Pilot Program and guidance from the Cyberinfrastructure Working Group (CIWG) it was confirmed that the operation of ONR vessels with few exceptions do not have Controlled Unclassified Information (CUI) DFARS 252.204-7012. CIWG agrees that CMMC level 1 is the best baseline moving forward.

NSF supports the continued need for a Cybersecurity Program to address the needs of the 18+ ships of the US Academic Research Fleet (ARF) in order to maintain the IMO Cybersecurity requirements.

Pilot Program Background

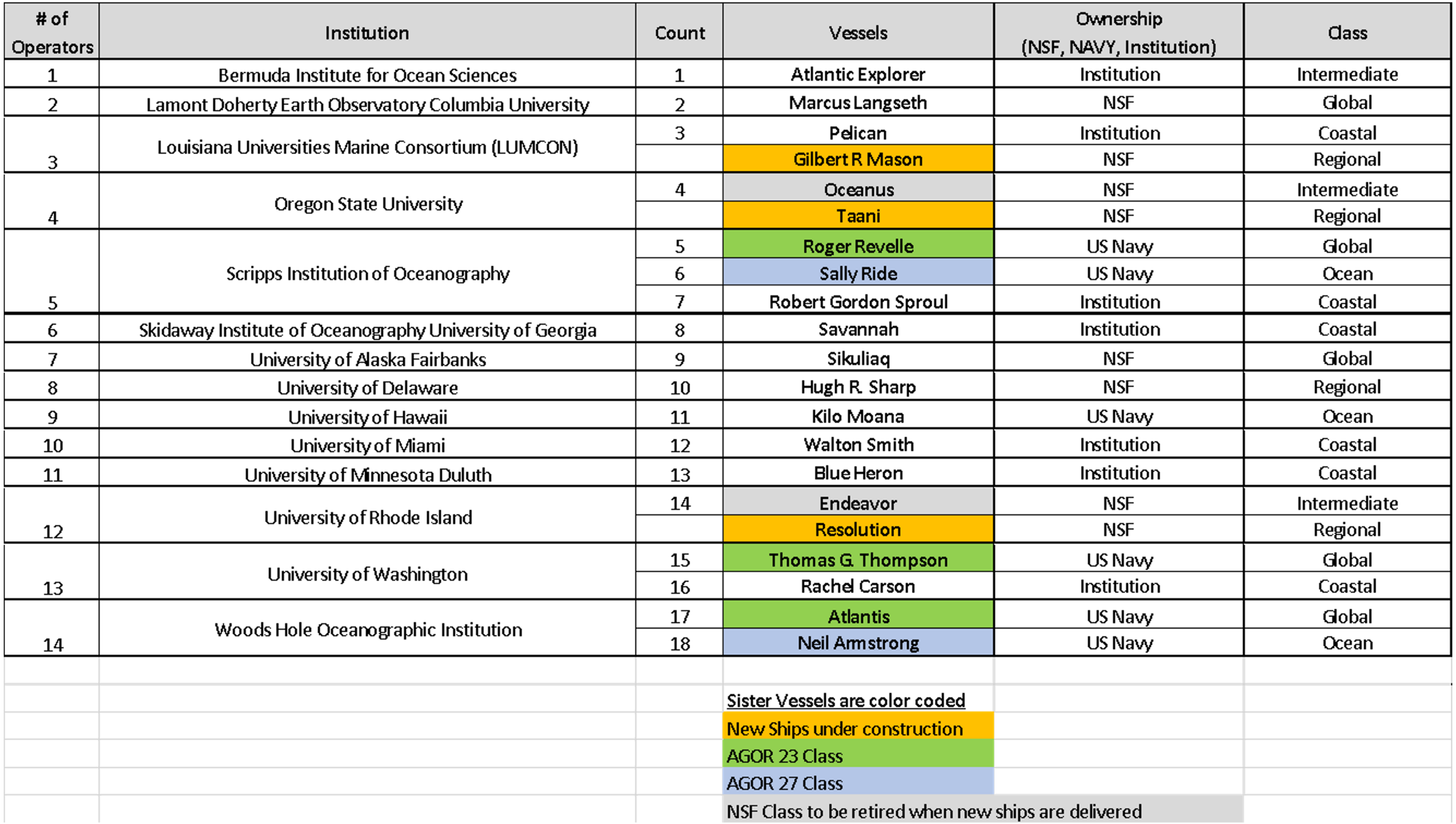
The scope of the work of the vendor has been to aid each Operator in maintaining cybersecurity compliance.

- Each Operator has a Cybersecurity Risk Management Plan (CRMP) in their Safety Management System (SMS).
- The intent of cybersecurity compliance is to reduce vessel vulnerability to cyber threats to both Information Technology (IT) and Operational Technology (OT) systems.

The scope of the Cybersecurity Program is for each vessel operator to maintain Compliance by updating the CRMP.

- The program will work with all ARF Operators to determine their specific CRMP updating needs.

Pilot Program



# of Operators	Institution	Count	Vessels	Ownership (NSF, NAVY, Institution)	Class
1	Bermuda Institute for Ocean Sciences	1	Atlantic Explorer	Institution	Intermediate
2	Lamont Doherty Earth Observatory Columbia University	2	Marcus Langseth	NSF	Global
3	Louisiana Universities Marine Consortium (LUMCON)	3	Pelican	Institution	Coastal
			🟧 Gilbert R Mason	NSF	Regional
4	Oregon State University	4	⬜ Oceanus	NSF	Intermediate
			🟧 Taani	NSF	Regional
5	Scripps Institution of Oceanography	5	🟩 Roger Revelle	US Navy	Global
		6	🟦 Sally Ride	US Navy	Ocean
		7	Robert Gordon Sproul	Institution	Coastal
6	Skidaway Institute of Oceanography University of Georgia	8	Savannah	Institution	Coastal
7	University of Alaska Fairbanks	9	Sikuliaq	NSF	Global
8	University of Delaware	10	Hugh R. Sharp	NSF	Regional
9	University of Hawaii	11	Kilo Moana	US Navy	Ocean
10	University of Miami	12	Walton Smith	Institution	Coastal
11	University of Minnesota Duluth	13	Blue Heron	Institution	Coastal
12	University of Rhode Island	14	⬜ Endeavor	NSF	Intermediate
			🟧 Resolution	NSF	Regional
13	University of Washington	15	🟩 Thomas G. Thompson	US Navy	Global
		16	Rachel Carson	Institution	Coastal
14	Woods Hole Oceanographic Institution	17	🟩 Atlantis	US Navy	Global
		18	🟦 Neil Armstrong	US Navy	Ocean

Sister Vessels are color coded

🟧 New Ships under construction

🟩 AGOR 23 Class

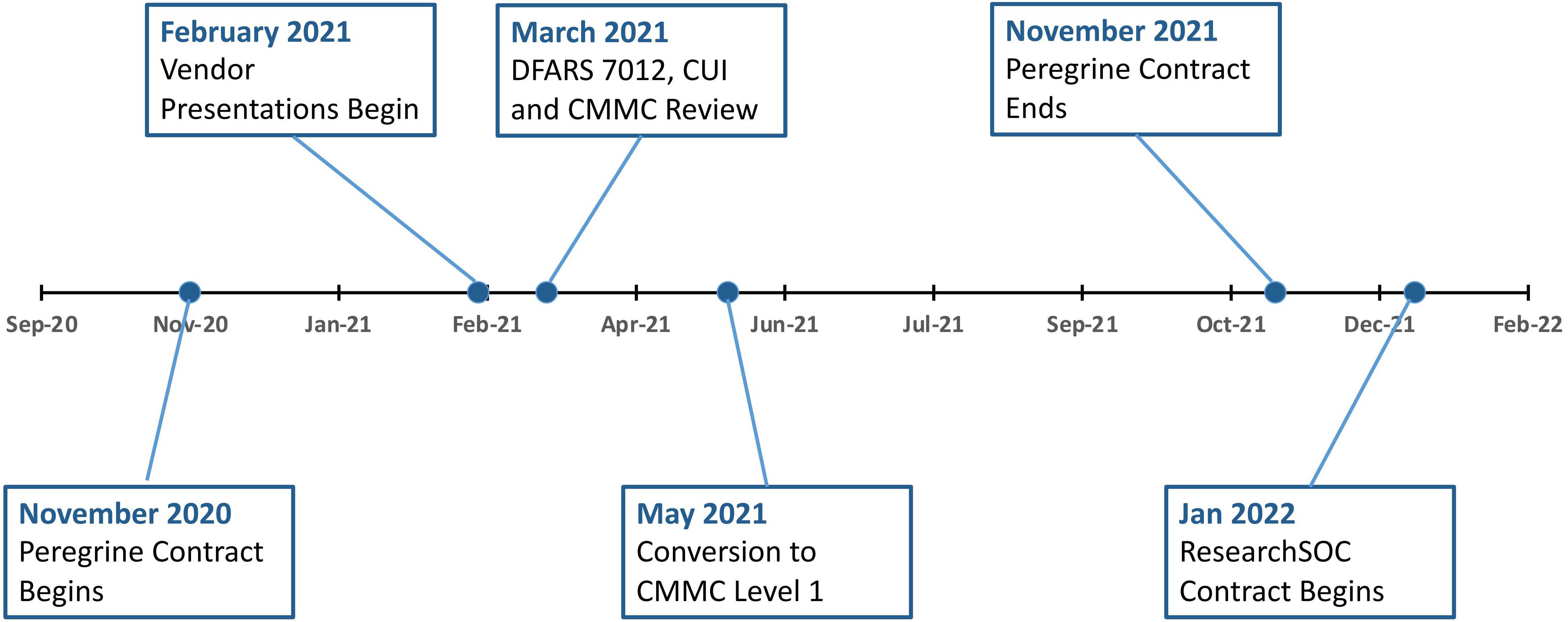
🟦 AGOR 27 Class

⬜ NSF Class to be retired when new ships are delivered

CMMC Level 1

- Consists of 17 Practices
- Focus is to safeguard federal contract information
- Requires an organization to perform specified practices
- Consists only of practices that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21

Timeline



February 2021
Vendor Presentations Begin

March 2021
DFARS 7012, CUI and CMMC Review

November 2021
Peregrine Contract Ends

November 2020
Peregrine Contract Begins

May 2021
Conversion to CMMC Level 1

Jan 2022
ResearchSOC Contract Begins

ResearchSOC

Research Security Operations Center (ResearchSOC) is an NSF-funded collaborative security response center that addresses the unique cybersecurity concerns of the research community.

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).

ResearchSOC Year 1

Statement of Work Highlights

1. ResearchSOC – OmniSOC 24/7 monitoring and alerting
2. Vulnerability Identification Service
3. Virtual Chief Information Security Officer (vCISO)
4. Virtual Security Team
5. Red Phone IR Service

The scope of ResearchSOC services for 1 year are targeted at accelerating the establishment of a Cybersecurity program for the ARF.