OOI Request for proposal: Cybersecurity vCISO team resources

Version 1-00
Document Control Number 2100-00001
2024-07-17

Woods Hole Oceanographic Institution
Woods Hole, MA. 02543
www.whoi.edu

In Cooperation with

University of Washington
Oregon State University

Document Control Sheet

Version	Date	Description	Originator
1-00	07/17/2024	First release	Jeffrey Glatstein

TABLE OF CONTENTS

WHO WE ARE

Woods Hole Oceanographic Institution (WHOI) assumed the duties of the Program Management Office (PMO) for the Oceans Observatories Initiative (OOI)[1] in October of 2018. The PMO is tasked with evaluating cybersecurity resources to implement the next stages of its cybersecurity program across OOI. The PMO is exploring the marketplace to retain services that deliver vCISO or team-based cybersecurity resources to provide to the PMO the expertise and resources needed to implement and harden OOI's next generation cybersecurity program.

OOI MISSION

The National Science Foundation's (NSF) Ocean Observatories Initiative (OOI) is an integrated infrastructure program composed of science-driven platforms and sensor systems that measure physical, chemical, geological and biological properties and processes from the seafloor to the air-sea interface.

The OOI network was designed to address critical science-driven questions that will lead to a better understanding and management of our oceans, enhancing our capabilities to address critical issues such as climate change, ecosystem variability, ocean acidification, geological events, and carbon cycling.

The OOI has transformed research of the oceans by integrating multiple scales of globally distributed marine observations into one observing system and allowing for that data to be freely downloaded over the internet in near-real time. The OOI will continue to deliver data and data products for a 30 year plus time period within an expandable architecture that can meet emerging technical advances in ocean science. It is important to note that OOI data is freely available to the public. OOI does not receive revenue by its use.

Building on last century's era of ship-based expeditions, recent technological leaps have brought us to the brink of a sweeping transformation in our approach to ocean research – the focus on expeditionary science is shifting to a permanent presence in the ocean. As technological advances continue over the lifetime of the OOI, developments in sensors, computational speed, communication bandwidth, Internet resources, miniaturization, genomic analyses, high-definition imaging, robotics, data assimilation, modeling and visualization techniques will continue to open new possibilities for remote scientific inquiry and discovery.

OOI is funded by the National Science Foundation and is managed and coordinated by the OOI PMO at the Woods Hole Oceanographic Institution (WHOI), in Woods Hole, MA. WHOI is also responsible for the Coastal Pioneer Array and two Global Arrays (Coastal and Global Scale Nodes – CGSN). The University of Washington is responsible for the cabled seafloor systems and moorings at the Regional Cabled Array (RCA). Oregon State University is responsible for the Coastal Endurance Array (EA) and for the CI Data Center housing the hardware and network, storing and processing the collected data.

[1] https://oceanobservatories.org/about/

REQUEST FOR PROPOSAL

PURPOSE

The intent of this RFP is to gather information and costs regarding the services an organization can provide in building the OOI cybersecurity program for a one year period of time. For the purpose of this RFP, services are meant to include:

- vCISO and supporting resources.
- Resources available with the necessary skill sets to meet OOI cybersecurity requirements inclusive of document authorship, reporting, table top exercises, log analysis and vulnerability testing.
- Knowledge and ability to implement CIS implementation groups 1 and 2.
- Method of tracking engagement and planning out deliverables for the period of performance.

TIMELINE

The RFP process schedule is outlined below. During the active time of this RFP, OOI will make resources available to answer questions by email.

Schedule

Milestone	Date
RFP Release	8/2/24
Submission of written questions from prospective offerors.	8/12/24
WHOI PMO responses to written questions. Each question with the response will be published to all candidates without attribution to the organization posing the question.	8/14/24
RFP Vendor Responsive Proposals	8/21/24
Schedule of Vendor interviews	8/26/24 – 8/30/24
Evaluation and Decision	9/6/24

HOW TO SUBMIT RFP QUESTIONS

Questions can be submitted by sending an email to jglatstein@whoi.edu with a subject of Cybersecurity RFP question. All answers will be emailed back to the full vendor list. OOI responses will be anonymized to preserve vendor privacy.

HOW TO RESPOND

All responses should be emailed to jglatstein@whoi.edu with a subject of Cybersecurity vCISO RFP response. Documents should be in a PDF format and contain an engagement approach, team detail along with a proposed cost structure.

Any and all costs incurred by an offeror in conjunction with the development of a response to this RFP are at the discretion of and are the sole responsibility of the offeror. WHOI shall not be liable for any expenses the offeror incurs in the preparation of its proposal in response to this RFP.
All proposals must be signed by an individual authorized to bind the offeror to the provisions of the RFP and to accept the award if selected. A proposal received after the date and time set for receipt of offers will not be considered. If an amendment to the RFP is required, it will be provided to each candidate.

CURRENT ENVIRONMENT

SUMMARY

The current OOI cybersecurity posture is considered effective but needs work in the development of policies and plans (e.g. incident response plan) as well as being extended to the program's subawardees. OOI cybersecurity efforts have primarily focused on the Data Center located at Oregon State University where the majority of the OOI cyberinfrastructure and data processing occurs. As the program has matured and the NSF focus on cybersecurity has increased, the scope of the cybersecurity program has grown to include data entry points at the Marine Implementing Organizations (MIO) subawardees. The MIOs are responsible for gathering and packaging the data received from the in-situ instruments in the water and sending them to the central data repository. Initial scope will not include securing the instruments or any equipment that falls under the control of the home MIO's cybersecurity departments. The plan is to implement CIS IG1 controls at the MIOs and IG2 controls at the Data Center.

EVALUATION

REQUIREMENTS

The winning organization will work with the OOI PMO and MIO Security Leads to:

- Author all appropriate documentation and policies (e.g. defense policy, audit log management, incident response…).
- Compile inventory lists and implement update strategies.
- Coordinate cybersecurity task activities across the MIOs.
- Provide skillset augmentation to understaffed or less trained personnel at MIOs.
- Assist in implementation of IG1 controls across the subawardees and IG2 at the Data Center.

- Author and present Quarterly and Monthly security reports to the PMO and Principal Investigators (Executive Leadership).
- Participate in tabletop exercises for disaster recovery (MITRE) to ensure resilience.
- Assist in vulnerability assessment and testing approaches.

RESPONSE

A winning response will clearly outline an acceptable approach to meeting the requirements. Timelines and an outline of hours per week and how those are utilized among tasks and objectives is essential. Make-up of the team's skill sets and how it will engage with OOI should be discussed. It is very important to OOI that the team presented and the accompanying cost proposal incorporates an opportunity for the team to become familiar with OOI as an organization and use that familiarity to provide informed solutions.

WHOI will issue to the successful offeror an agreement consisting of the statement of work; specific terms required under our NSF funding agreement and that establish the agreement's duration, pricing, reporting hours and invoices, and payment; and WHOI's standard terms and conditions.

WHOI's terms and conditions can be found here https://www.whoi.edu/fileserver.do?id=280984&pt=10&p=120155.

Refer to 2 CFR Part 200, Appendix II, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, to review the specific terms required for subcontracts under WHOI's NSF-issued Cooperative Agreement.

Evaluation criteria to be used is:

- Method of engagement (e.g. subscription or time and materials).
- Overall approach to the implementation of a cybersecurity program (e.g project plans, task management, and determination of priorities).
- Knowledge of CIS controls, in particular implementation groups 1 and 2.
- Ability to bring resources to the project that enhance the OOI skill.
- Track record of successful engagements similar to OOI.
- Flexibility in the application of hours week to week.
- Team stability

MEASUREMENTS OF SUCCESS

A successful relationship based on the proposed approach will be measured by the extent to which it appears most likely to promote and achieve the following:

- Develops a clear list of yearly milestones working with the PMO and Security Leads.
- Adopts a measured/prioritized approach with a list of tasks and timelines to meet milestones.
- Provides clear communication with the Senior Manager of Cyberinfrastructure and the Project Manager of the Data Center.
- Provides guidance on new threats with a risk assessment that will be incorporated and updated through the OOI risk register.
- Successful implementation (working with OOI resources) of CIS IG1 and IG2 within a year.
- Authors plans and policy with a priority on incident response and disaster recovery.
- Develops a full asset inventory across the program (working with OOI resources).
- Reports out on at least one incident and disaster recovery table top exercise.
- Working with OOI resources, ensures OOI has the reference documentation in place to inform an outside review of the scope and completeness of OOIs cybersecurity program.