7.10 – Cyber Risk Management (CRM) Instructions

Originator:	Approved By:
Hank Ayers	Timothy Twomey

20.1 GENERAL OVERVIEW

Interconnected computer based systems on vessels have the possibility for attacks to affect personnel data, human safety, the safety of the vessel, and to threaten the marine environment. Attackers may target any combination of people and technology to achieve their aim, anywhere where there is a network connection. Safeguarding shipping from current and emerging threats involves a range of measures that are continually evolving. It is necessary to achieve a common set of minimum functional and performance criteria in order to deliver a whole system that can indeed be described as cyber resilient.

The purpose of this chapter is to provide a set of general requirements for cyber resilience on board WHOI's vessels and to implement technical means and procedures which would lead to cyber resilient vessels that can be maintained throughout their service life. Specific means and procedures shall be outlined in a **Cyber Risk Management Plan (CRMP).**

The requirements contained in this chapter apply to:

- **Information Technology (IT**) systems on board ships, i.e. computer-based devices, software and associated networking focusing on the use of data as information, and;
- **Operational Technology (OT)** systems onboard ships, i.e. those computer-based systems using data to control or monitor physical processes, critical propulsion, navigation, steering equipment, etc. that can be vulnerable to cyber incidents and, if compromised, could lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

Risks to critical cyber-enabled systems are contributed to by three fundamental properties: (1) the safety impact of a failed system on the vessel; (2) vulnerabilities presented in the design of digital networks connecting those systems and the accessibility of related digital endpoints; and, (3) the threats presented by the lack of trust assignable to each person and digital device that can access the digital endpoints. A risk-based CRMP provides protections that mitigate identifiable risk contributions by means of procedures, technologies, and supporting management programs, with each protection being directly traceable to a specific risk contribution.

20.2 REGULATIONS, STANDARDS AND GUIDELINES

The following regulations, standards and guidelines have been considered:

- IMO Resolution MSC.428(98) "Maritime Cyber Risk Management in Safety Management", June 2017
- IMO MSC-FAL.1/Circ.3, "Guidelines on Maritime Cyber Risk Management", July 2017
- "Framework for Improving Critical Infrastructure Cybersecurity", version 1.1, National Institute of Standards and Technology (NIST), April 2018
- "The Guidelines on Cyber Security On-board Ships", v4, BIMCO, CUA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL, December 2020
- USCG Reporting Suspicious Activity and Breaches of Security CG-5P Policy Letter 08-16.
- ABS -THE APPLICATION OF CYBERSECURITY PRINCIPLES TO MARINE AND OFFSHORE OPERATIONS Cybersafety Volumes 1 and 2

Each of the above is available electronically via the internet and should be monitored for updates and revisions.

20.3 DEFINITIONS AND ABBREVIATIONS

The following definitions and abbreviations apply to this chapter:

Adware: Also called pop-up ads, these are advertisements that appear in their own window in a browser. These may be harmless but can contain computer viruses.

Bot: Malware that allows an attacker to make use of an affected computer.

Controlled Unclassified Material (CUI): CUI is controlled information set by the Program Contracting Officer. Typically, will be noted with a Distribution statement.

Covered Defense Information (CDI): CDI is a subset of Controlled Unclassified Information (CUI). CDI is provided to a contractor by the DoD, and it becomes the responsibility of the contractor to protect the security and integrity of the information. CDI has four subcategories, controlled technical information (CTI), operations security information, export-controlled information, and other marked information that requires protection.

Cyber Attack: Any type of offensive maneuver that targets vessel's systems (both IT and OT networks), computer networks, and/or personal computer devices. The goal of an attack is to compromise, destroy or access systems and data belonging to the company and vessel.

Cyber Incident: An event resulting from any cyber-attack action, either intentional or unintentional, that targets systems on board, which actually or potentially results in adverse consequences to an on-board system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences.

Cyber Resilience: The capability to reduce the occurrence and mitigating the effects of incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a vessel, which potentially lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

Cybersecurity: The protection of IT and OT systems, information and data from unauthorized access, manipulation and disruption.

Information Technology (IT): Devices, software and associated networking focusing on the use of data as information, as opposed to Operational Technology (OT).

Key Loggers: Either physical devices or software that track all use of the keyboard and store it into a log. Key loggers can be discreetly plugged into USB ports or can be transferred onto a system through a compromised USB drive.

Malware: Any software that is used to attack a network or system, gather sensitive information or gain access to secure areas. Email is the most common method of spreading malware.

Operational Technology (OT): Devices, sensors, software and associated networking that monitor and control on board systems. OT systems may be thought of as focusing on the use of data to control or monitor physical processes.

Password Guessing Attack: The identification of a password of a legitimate user to gain access to a system.

Phishing: A type of social engineering involving spam emails (often sent to a large number of recipients at random) that are designed to "fish" for sensitive information such as bank details and passwords. Phishing emails often contain infected links or attachments. The emails can vary in quality and they may look official or they can be poorly worded/designed. They are designed to initiate a response so that the attackers exploit the individual concerned. They are often used to gain access to networks. By infecting the receiver, a gateway into their network is created and then used to further exploit and take over the other systems.

Ransomware: A form of malware that restricts access to the systems it infects, encrypting data so that data cannot be accessed or used. Ransomware is often designed to threaten publication or destruction of a user's data and will usually not unencrypt data until a large ransom is paid, often within a time limit. Sometimes, even if the ransom is paid, the data may never be unencrypted.

Social Engineering: The deliberate manipulation of people to gain unauthorized access to data, applications or systems. It typically involves tricking a person into divulging sensitive or confidential information, or providing access to IT or OT networks, and it usually takes place via a malicious hyperlink or attachment contained within an email.

Spear Phishing: A phishing email attack that involves an email to a specific recipient that appears to be from a trusted or known source, often from within the recipient's own email address book.

Spoofing: Involves visiting a website that is pretending to be a legitimate website or visiting a website that has been hijacked. On a hijacked website, links can be changed or compromised and systems infected without the user's knowledge.

Spyware: Software that "spies" on a computer and can capture information such as web browsing habits, emails, user names, passwords and credit card information.

Trojan: Malware that disguises itself as legitimate software but is actually designed to retrieve sensitive or confidential data.

Virtual Private Network (VPN): A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks utilizing tunneling, security controls and endpoint address translation giving the impression of a dedicated line.

Viruses: Malware in the form of small programs or scripts designed to negatively affect the health of systems or networks. Viruses can create, move or erase files and disrupt a computer's memory of start-up systems.

Worms: Similar to viruses, but designed to infect and spread to multiple systems or computers.

20.4 CYBERSECURITY POLICY

WHOI recognizes that the IT/ OT systems on board its vessels may be exposed to cyber threats and have possible vulnerabilities which, if left unmitigated, may intentionally or inadvertently be avenues to corrupt or compromise the IT/OT systems. This, in turn, has the potential to adversely affect the safety of the crew, the vessel, other property, or the marine environment.

WHOI further recognizes that threats can be presented by both malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions). In general, these actions expose vulnerabilities (e.g.

outdated software or ineffective firewalls) or exploit a vulnerability in operational or information technology.

WHOI appreciates that vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber discipline. In general, where vulnerabilities in operational and/or information technology are exposed or exploited, either directly (e.g. weak passwords leading to unauthorized access) or indirectly (e.g. the absence of network segregation), there can be implications for security and the confidentiality, integrity and availability of information. Additionally, when operational and/or information technology vulnerabilities are exposed or exploited, there can be implications for safety, particularly where critical systems (e.g. bridge navigation or main propulsion systems) are compromised.

It shall be the Cybersecurity Policy of WHOI to address these threats and vulnerabilities to the extent possible through a risk-based approach which is supported by five functional elements of Identify, Protect, Detect, Respond and Recover. The goal of this approach is to reveal gaps that can be addressed by procedural, physical, or other technological means, which will result in more cyber resilient vessels. The remainder of this chapter describes the general details of how WHOI’s Cybersecurity Policy will be supported. Specific details are outlined in the CRMP. This policy applies to all crew members on board the vessels managed by WHOI.

20.5 RISK ASSESSMENT

Risk assessment is essential to determine the most important factors needed to address cyber risks and to support prioritization of mitigating controls (countermeasures). The risk assessment helps select activities that reflect desired cyber resilience outcomes, giving the ability to dynamically select and directly improve cybersecurity risk management.

Risk assessments of both IT and OT shipboard systems shall be carried out by WHOI to understand the cybersecurity risks related to ship operations depending on IT/ OT systems. Threats and vulnerabilities shall be identified along with corresponding mitigating controls. The mitigating controls will be prioritized based on the severity of the risk of the threat or vulnerability.

During the operational life of the vessel, WHOI will update the risk assessments considering the constant changes in the cyber scenario and new weaknesses identified in IT/ OT systems onboard in a process of continuous improvement. Should new risks be identified, WHOI shall update existing, or implement new risk mitigation measures. In the risk assessment, the following elements shall be considered:

- Asset vulnerabilities shall be identified and documented.
- Identifying threat vectors, both internal and external, shall be documented.
- Cyber threat intelligence shall be applied, and information shall be received from information sharing forums and sources.
- Potential impacts on human safety, safety of the vessel and/or threat to the environment and likelihoods shall be identified.
- Threats, vulnerabilities, likelihoods, and impacts shall be used to determine risk.
- Possible effects related to integration of systems, or interfaces among systems, including systems not onboard (e.g. if remote access to onboard systems is provided), shall be considered.

Risk assessments for each vessel are included in the respective vessel CRMP.

20.6 FUNCTIONAL ELEMENTS

IMO Resolution MSC.428(98) "Maritime Cyber Risk Management in Safety Management", June 2017, states that a company's approved Safety Management System should consider cyber risk management in accordance with the functional requirements of the ISM Code. The IMO Resolution references 1MO MSC-FAL.1/Circ.3, "Guidelines on Maritime Cyber Risk Management", July 2017, which provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities.

The IMO Guidelines present **five functional elements** that support effective cyber risk management. These functional elements are not sequential, they are assessed concurrently and continuously in practice and incorporated appropriately in the vessel CRMP. The following are the five functional elements:

Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.

Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

These functional elements combine the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange and constitute an ongoing process with effective feedback mechanisms. The "Framework for Improving Critical Infrastructure Cybersecurity", version 1.1, National Institute of Standards and Technology (NIST), April 2018, (NIST Framework), incorporates these five functional elements and subdivides them into categories and subcategories, the basis of which is used by WHOI to identify requirements and to assign policies and procedures to strengthen the cyber resilience of WHOI 's vessels. These policies and procedures are generally outlined in the chapters that follow, organized by the five functional elements. Specific policies and procedures are outlined in greater detail in the CRMP.

20.6.1 IDENTIFY

20.6.1.1 General Overview

The requirements for the Identify functional element are aimed at identifying, on one side, the IT/ OT systems onboard, their interdependencies among them and the relevant information flows and, on the other side, the key resources involved in their management, operation and governance, their roles and responsibilities.

The activities in the Identify functional element are foundational for effective use of the NIST Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Categories within this functional element include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

20.6.1.2 Inventories

WHOI shall maintain and update inventories of the IT/ OT systems and their relevant software used on board its vessels. The hardware and software inventories will be maintained in the vessels CRMP.

For hardware, the inventory shall contain at least the following information:

For each IT/ OT system, technical features (brand, manufacturer, model, main technical data) and specific function;

A block diagram identifying the logical and functional connections among various IT/ OT systems onboard and between the systems and external devices or networks, the topology of networks connecting the systems and the intended function of each node;

For network devices such as switches, hubs, gateways etc., a description of the connected subnetworks, IP ranges, MAC addresses of nodes connected (or addresses/identifiers specific to the protocols used in the network);

The main features of each network (e.g. protocols used) and communication data flows in all intended operation modes;

A map describing the physical layout of each digital network connecting the IT/ OT systems onboard, including the physical location of the systems onboard, the paths of network cables (for wired networks) or the position of wireless transmitters and receivers (for wireless networks), and the physical location of network access points.

For software, the inventory shall contain at least the following information, for each software application program, operating system, firmware, etc.:

The IT/ OT system where it is installed, a short description of its purpose, technical features

(brand, manufacturer, model, main technical data) and specific function;
Application, version information and file location;

20.6.1.3 Roles and Responsibilities

The following roles and responsibilities are defined as follows:

- The Master is assigned as the Cybersecurity Officer on board. The Master is responsible to ensure that the crew is familiarized and trained with regard to basic cybersecurity awareness and good cyber hygiene practices. The Master shall report any event which could be considered a possible cyber-attack or any technical issues with regard to IT/ OT systems and their respective software installations to the Director of Ship Operations (DSO) and WHOI IS Department. The Master shall be responsible for maintaining the list of passwords associated with the IT/ OT systems on board the vessel. The Master is to ensure good cyber hygiene is being maintained on board the vessel to reduce the possibility of a cybersecurity event from occurring.

- The WHOI IS Department shall be responsible for maintaining the IT systems on board the vessel with regard to hardware and software maintenance, repairs and updates. They shall maintain an inventory of the IT systems and relevant software on board each vessel. They shall implement user access policy of the IT systems on board. They shall monitor the IT systems on board the ships for any activity which could be deemed a cyber-attack or incident.

- The Chief Engineer shall be responsible for maintaining the OT systems on board the vessel with regard to hardware and software maintenance, repairs and updates. They shall maintain an inventory of the OT systems and relevant software on board each vessel.

- The Cybersecurity Committee shall be comprised of at least one member of the WHOI IS, Master, Chief Engineer, WHOI Cybersecurity Officer and the WHOI Designated Person Ashore. The Committee, as a whole, shall be responsible for preparation and maintenance of the cyber risk assessments and the vessel cybersecurity plans. The Cybersecurity Committee shall meet regularly to discuss cyber threats and vulnerabilities, and to prioritize the mitigating controls to be put into place to reduce the risks associated with these.

20.6.1.4 Vessel Cybersecurity Assessment

WHOI's fleet shall have conducted a vessel cybersecurity assessment. The purpose of the assessment is to identify of IT/ OT systems, the existing cyber threats, and vulnerabilities specific to the ship. The identified cyber threats and vulnerabilities and proposed recommendations will be considered by the Cybersecurity Committee with the goal of enhanced cyber resilience for WHOI 's vessels.

20.6.2 PROTECT

20.6.2.1 General Overview

The requirements for the **Protect** functional element are aimed at the development and implementation of appropriate safeguards supporting the ability to limit or contain the impact of a potential cybersecurity event. Areas covered by these requirements include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; Protective Technology. For details on the below mentioned items, refer to the CRMP.

20.6.2.2 Separation of Networks

To the extent possible, networks connecting on board IT/ OT systems shall be separated into security zones with well-defined control policy and security features. Networks belonging to security zones with different control policies shall be logically and physically separated and segregated. In other words, the crew system network shall be separate from the vessel's business IT system network, which shall be separate from the Science side network, which shall be separate from the vessel's OT system network.

20.6.2.3 Familiarization and Training

Crew members shall be initially familiarized in aspects of cybersecurity by being provided with a cybersecurity familiarization sheet as part of their sign-on package. Additional familiarization and training shall be a topic of discussion during the monthly safety and environmental meetings held on board. The vessel shall also be provided with a training video relating to cybersecurity awareness.

20.6.2.4 Antivirus and Malware Protection

Antivirus and protection from malicious code shall be established and kept up to date for the systems on board. Use of external systems on all vessels shall be restricted by a web filtering system.

20.6.2.5 Physical Access Control

IT/ OT systems on board shall be provided with physical access control. They shall be maintained in locked restricted areas, i.e. the bridge, the engine control room, electrical and propulsion equipment rooms, or locked cabinets. Access to these spaces shall be limited to the crew or escorted visitors with official ship's business.

Business IT systems may be located in crew offices, dayrooms, and staterooms. The doors for these spaces shall be kept locked when the occupant is out of the space, or the systems must be screen locked to prevent unauthorized use.

20.6.2.6 Logical Access Control

IT systems on board shall be provided with logical access control in the form of distinct usernames and passwords. This also includes WIFI access onboard. Username and password logins shall be required and systems shall "time out" after a prescribed unattended period, requiring the user to log back in. Generic usernames such as "user" and generic/default passwords such as "password", "12345", or the like shall not be used.

Usernames and passwords shall not be openly displayed. The Master shall be responsible for maintaining a list of usernames / devices and their associated passwords, and access to this list shall be restricted. A copy of the list is to be maintained by WHOI’s IS Department and an updated copy provided if there are any changes.

Passwords shall not be shared in turnover notes or with any person not authorized to use a specific computer. Access to external systems on the internet shall be limited to computers as determined by the Master. The installation of software onto company computers shall be restricted to those with administrative rights. Logical access control with regard to OT equipment is only available to authorized third party service technicians to perform required maintenance, system troubleshooting, repairs and upgrades.

20.2.6.7 Remote Access Control

Remote connections to IT/ OT systems and equipment shall be limited to WHOI staff as determined by the DSO and WHOI IS Director.

20.6.2.8 Portable Media

All portable media devices on IT systems shall be shut down with exceptions permitted by the Master.

All portable media devices must first be scanned, on a dedicated separate computer not connected to the OT system or equipment, for viruses and malware prior to being used on OT equipment. Dedicated USB devices for items like Electronic Chart Display and Information System (ECDIS) updates should be utilized.

Personal USB devices or similar storage devices should not be used on shipboard systems at any time. Same requirements apply to outside vendors working on any shipboard systems.

20.6.2.9 Software and Firmware Updates

OT systems shall have their software and/or firmware kept up to date by an authorized third-party service technician.

IT systems shall have their software and/or firmware kept up to date by the WHOI IS Department.

20.6.3 DETECT

20.6.3.1 General Overview

The Detect function enables timely discovery of cybersecurity events. Examples of outcome Categories within this function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes. For details on the below mentioned items, refer to the CRMP.

20.6.3.2 Cybersecurity Monitoring and Scanning

WHOI shall utilize cybersecurity monitoring and scanning software to allow for the timely discovery of possible cyber-attacks or incidents on IT equipment.

There are no systems in place that are able to monitor the OT equipment for a possible cybersecurity event. Detection is usually provided in the form of alerts or alarms from the particular piece of OT equipment. These alarms are the indication that the equipment is not functioning properly and must be investigated to determine the cause of the error. At that time, it may be determined that a cybersecurity event has occurred.

20.6.3.3 Crew Awareness

The crew shall be trained annually to recognize possible cyber-attacks or incidents. They should know the signs when a computer may have been compromised as listed below:

an unresponsive or slow to respond system
unexpected password changes or authorized users being locked out of a system
unexpected errors in programs, including failure to run correctly or programs running unexpectedly
unexpected or sudden changes in available disk space or memory
emails being returned unexpectedly
unexpected network connectivity difficulties
frequent system crashes
abnormal hard drive or processor activity
unexpected changes to browser, software or user settings, including permissions

In the event the crew notices any of these signs, they must report the possibility of a cybersecurity incident to the Master.

In regards to a possible cybersecurity event with the OT equipment, it will be most noticeable to the crew who use this equipment on a daily basis. In the event OT equipment is found to be functioning improperly due to unknown errors, it should be immediately reported to the Chief Engineer and Master for further investigation.

All WHOI employees are required to complete cybersecurity online training via the WHOI Environment Health & Safety (EH&S) Training Management System. Training Modules are assigned to individual employee profiles. Officers and other key positions may be assigned other computer-based training per direction from Ship Operations.

20.6.4 RESPOND

20.6.4.1 General Overview

The Respond function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

20.6.4.2 Shipboard Response

With regard to IT equipment, crew members shall respond to any potential cybersecurity incidents by promptly reporting same to the Cybersecurity Officer (the Master) on board, who in turn shall promptly report it to the WHOI IS Department and the DSO. The Master shall be guided accordingly by the WHOI IS Department and/or the DSO in regards to the appropriate action to be taken to mitigate the cybersecurity event. If the network is compromised in a way that doesn't allow the Master to send an email or if it is determined to be an urgent matter, then a phone call should be made to the DSO.

With regard to OT equipment, crew members shall respond to any potential cybersecurity incidents by promptly reporting same to the Cybersecurity Officer (the Master) on board, who in turn shall promptly report it to the DSO. The DSO shall consult with third party equipment service technicians as needed. The Master shall be guided accordingly by the DSO as to the appropriate action to be taken to mitigate the cybersecurity event until shoreside assistance can be provided if needed.

The reporting of any incident should be done via email or if it is determined to be an urgent matter then a phone call should be made to the DSO. The following reporting will occur in event of a cybersecurity incident:

Any significant cyber event is to be reported immediately by the DSO to the National Cybersecurity and Communications Integration Center (NCCIC) at (888) 282-0870 in accordance with CG-5P Policy Letter 08-16.

The DSO will also notify Class, Local COTP, Port State, Program Manager from Office of Naval Research (ONR), Program Manager of National Science Foundation (NSF) and WHOI Senior Management as appropriate.

The DSO will also inform the WHOI Information System Security Manager (ISSM). The ISSM is responsible for reporting into Defense Industrial Base Cyber incident reporting portal (DIBNet) as required.

Defense Federal Acquisition Regulation Supplements (DFARS) within the vessel Charter Party Agreements (CPA) may include the following below and are covered via the ISSM reporting appropriately.

> DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
> DFARS 252.239-7010 Cloud Computing Services
> FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

20.6.5 RECOVER

20.6.5.1 General Overview

The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome categories within this function include: Recovery Planning; Improvements; and Communications.

20.6.5.2 Shipboard Recovery Plan

With regard to IT equipment, the Cybersecurity Officer (the Master) on board shall coordinate all recovery efforts after an apparent cyber incident with the DSO and WHOI IS Department. There is redundancy of communications and other IT equipment which will allow for continued functionality until the equipment can be fully restored.

With regard to OT equipment, the Cybersecurity Officer (the Master) on board shall coordinate all recovery efforts after an apparent cyber incident with the Port Engineer, Chief Engineer and the DSO. The Port Engineer shall coordinate with the Chief Engineer and DSO (as appropriate) in order to consult with third party equipment service technicians as needed and remote and/or on-board services shall be arranged accordingly. There is also redundancy of OT equipment onboard in the event of a failure due to the likelihood of not being able to provide shoreside repair service in a timely manner if the vessel is at sea. This can be found with vital navigation equipment such as Radars, ECDIS, GPS, Propulsion and Control systems.

Related Documents:

Cyber Risk Management Plan (CRMP) - R/V Neil Armstrong

Cyber Risk Management Plan (CRMP) - R/V Atlantis

Compliance to CMMC Level 1, WHOI Ship Operations (Port office, AGOR 25, AGOR 27)