A Review of the Maritime Cybersecurity Regime Over the Last Decade

Leigh Armistead
Peregrine Technical Solutions, Juneau, Alaska, USA

leigh.armistead@goldbeltfed.com

Abstract: This paper discusses the development of how the Maritime Cybersecurity regime has evolved over the last decade due to new instructions, mandates, doctrine and criteria that has been established to better protect both the traditional Internet Technology (IT) assets as well as the Industrial Control Systems (ICS). The methodology of this paper is to layout the new regulations over the last 10 years, and to showcase how these mandates affect operational issues at sea. The key factor, that will pervade all of the discussions of cybersecurity in the maritime domain, is the intense focus on safety, only to be followed by availability. This is unique, as the IT sector traditionally is focused on confidentiality, but Operational Technology (OT) or Facility Related Control Systems (FRCS) are a different set of systems, which require continuous operation, hence the need to always be on. In addition, the author will lay out in a systematic function, all of the new regulations in the last 10 years, why they were needed, and how did they change the training, skillsets, as well as processes that have been implemented to ensure compliance moving forward. Peregrine Technical Solutions, LLC. (Peregrine) is led by Dr Leigh Armistead, CISSP, who has conducted a number of maritime cybersecurity same tasks since 2014. It is a small business, based in Juneau, Alaska (US), specializing in ICS/OT/FRCS cybersecurity, where we have successfully conducted assessments over the last decade for the US Department of Defense (DoD) as well as academia. We are currently the prime contractor for the US Coast Guard Advanced Metering Systems, and we won an Army contract in 2023 for Facility Related Control Systems (FRCS) cybersecurity. From 2017-2021, we were the lead for the Platform Resilience Mission Assurance (PRMA) for the DoD, plus we have the first Cybersecurity Department of Labor Registered Apprenticeship Program (RAP) in the nation for adults (2016) /Youth Registered Apprenticeship (YRA) (2019). Dr Leigh Armistead was a member of the NATO project, SAS-163, Energy Security in the Era of Hybrid Warfare. This paper is a series of case studies of contracts and research efforts that Peregrine staff conducted over the last decade. It lays out a series of scenarios, using action research, as part of a qualitative methodology, to demonstrate the changes for the maritime community from a cybersecurity aspect. As this is a series of operational actions, there is not a literature review as such but instead, we abide by regulations, mandates, instructions and notices that are issued by a variety of regulatory bodies and organizations. The key participants are as follows: International Maritime Organization (IMO) – Regulatory Body. Peregrine Technical Solutions – FRCS Cybersecurity Provider. Academic Research Fleet (ARF) – 18 Ships. National Science Foundation (NSF) – Contract Sponsor. University of California San Diego (UCSD) – Original Organization requesting Support. Woods Hole Observatory Institute (WHOI) – Follow-on Contract Sponsor

Keywords: Cybersecurity, Maritime, ICS, FRCS, OT

1. Initial Cyber Security Efforts

In June 2017, the International Maritime Organization (IMO) released a Maritime Safety Committee (MSC) resolution that addresses Maritime Cyber Risk Management in Safety Management Systems (MSC-FAL.1/Circ. 3). This resolution "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". The resolution also 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." This was the first time that ships and their crew were directed to abide by a cybersecurity requirement, and it gave the community over three years to be ready to meet this deadline. Of note, these new requirements were embedded as a safety issue, which meant they were not ignored (as much), and needed to be met to pass the inspection.

Peregrine was requested, starting in 2018 to help the University of California of San Diego (UCSD) to meet this requirement. Over a two-year period, these subject matter experts (SMEs) developed a series of recommendations and in October 2020, a contract was let from the National Science Foundation (NSF) to support all 14 Universities of the Academic Research Fleet (ARF) which is comprised of 18 ships across the United States. We started a series of cybersecurity efforts on 20 November 2020 and conducted over a year long period to satisfy the MSC-FAL.1/Circ. 3 mandate, based on these key elements below:

- Identify: Define personnel roles and responsibilities for Cyber Risk Management (CRM) 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. Update procedures for reporting non-conformities, accidents, and hazardous situations to include reports relating to cyber incidents.
- 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. Ensure that adequate resources and shore-based support are available to support the Data Protection Act in responding to the loss of critical systems.
- Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event. Include creation and maintenance of back-ups into the ship's operational maintenance routine.

Our team conducted at the height of COVID, a robust and comprehensive cybersecurity effort where we gave bonus support not requested in the original RFP, specifically for the six Navy-owned ships, that had immediate Defense Federal Acquisition Regulation (DFARS) 252.204-7012 requirements, where we supplied the 10 required files, plus conducted table-top exercises with the staffs at Woods Hole Observatory Institute (WHOI), University of Hawaii (UH), University of California San Diego (UCSD) and University of Washington (UW). Our customer was extremely happy that we went above and beyond the contracted deliverables by doing things such as delivering detailed HW/SW inventories for each ship and attending American Bureau of Shipping (ABS) inspections virtually, so that we could answer all questions regarding cyber security for each ship. On that original 2020-2021 effort, from our interviews with the staff of the 14 Universities and there was a wide variety of knowledge and expertise. Some of the larger Universities, had a relatively strong cyber security posture, with no Information Technology (IT) / Operational Technology (OT) overlap meaning that it is unlikely that a threat actor could damage ship operations remotely. On others, not so much, as we found that there is a large amount of network segmentation on the ships from the larger Universities, where science equipment is separated from other devices. And in virtually instances, the ships crew did not have a current list of all of their equipment, which we provided as part of this contract.

The goal of these assessments was to analyse and assess the ship's network, its systems/devices to identify any vulnerabilities that could compromise or result in either loss of confidentiality, loss of integrity, or result in a loss of operation of the equipment, system, network, or even the ship. These vulnerabilities and weaknesses could fall into one of the following categories:

- Technical – software defects, End of Life (EOL) or End of Support (EOS) systems
- Design – access management, unmanaged network interconnections
- Implementation – errors such as misconfigured firewall rules or access control lists
- Procedural – system and physical access or other user errors

In addition, for this effort, Peregrine cybersecurity subject matter experts (SMEs) conducted these cyber ship assessments, in which the following items were completed:

- Map the ship's key functions and systems and assign potential impact levels using the Confidentiality, Integrity, and Availability (CIA) model, taking into consideration the operation of OT systems
- Identify main producers of critical shipboard IT and OT equipment
- Review detailed documentation of critical OT and IT systems including their network architecture, interfaces, and interconnections
- Identify cyber security points-of-contact with each of the producers and establish a working relationship with them
- Review detailed documentation on the ship's maintenance and support of the IT and OT systems
- Establish contractual requirements and obligations that the shipowner/ship operator may have for maintenance and support of shipboard networks and equipment
- Support the risk assessment with an external expert to develop detailed plans, including producers and service providers as necessary

2. Different Focus from Traditional Ashore IT Cyber Assessments

From a Maritime Cyber Security Implementation aspect, historically the ongoing, day-to-day operational efforts focused on availability, and to identify cybersecurity vulnerabilities for its potential impact and the probability of its exploitation immediately. Shown below are the recommended technical and/or procedural

corrective actions at a high-level that should be used, and ideally, there should be a cyber risk assessment for each identified vulnerability:

- Executive summary – a high-level summary of results, recommendations, and the overall security profile of the assessed ship
- Technical findings – breakdown of discovered vulnerabilities, their probability of exploitation, the resulting impact, and appropriate technical fix and mitigation advice
- Prioritized list of actions – the priorities allocated should reflect the effectiveness of the measure, the cost, the applicability, etc. It is important that this list should be a complete list of options available and not represent a list of services and products the third-party risk assessor, if applicable, would like to sell.
- Supplementary data – a supplement containing the technical details of all key findings and comprehensive analysis of critical flaws. This section should also include sample data recovered during the penetration testing, if any, and all critical or high-risk vulnerabilities.
- Appendices – records of activities conducted by the cyber risk assessment team and the tools used during the engagement.

As alluded earlier, the ARF engagement allowed the entire fleet to pass its yearly ABS inspection for cybersecurity over a four-year period starting in 2021. The activities performed during this previous onsite ship assessment included reviewing the configuration of all computers, servers, switches, routers, and other network enabled technologies, plus cyber security procedures and documentation for connecting and managing all available IT and OT systems and devices were also reviewed. In addition, the Peregrine SMEs also conducted a virtual assessment of the involvement of the crew of all levels; particularly the master, chief engineer and first mate. By doing this, the Peregrine team could better understand the implementation of the IT/OT systems onboard and how they may vary from stated or recommended design documentation. This assessment methodology also helped in understanding the level of cyber training delivered to the ship's crew.

Specifically, the Peregrine staff conducted passive IT/OT network scans, storing all data in a secure portal, specific to WHOI. Data collection devices were scrubbed after the data was transferred securely to the backup device so as to avoid any leakage of confidential data. Information and findings were transferred from the IMO Test Plan Template to the implementation working documents:

- Technical Findings Worksheet Template
- Supplementary Data Worksheet Template - Supports technical findings
- Appendices - Authoritative documents, requirements cited
- Findings were analyzed, and risks identified for mitigation based on criticality to personnel, operations, Confidentiality/Integrity/Availability (CIA) values, and mission assurance
- Customer Relationship Management (CRM) analysis performed; triaged risks identified in Risk Sheet Template
- Actions Worksheet Template sets out the outbound actions required to mitigate risk
- Management Implementation Begins

A key element of all sites was to understand the H/W and S/W of the various ships, and the Peregrine cybersecurity SMEs, in which the following items were completed:

- Map the ship's key functions and systems and assign potential impact levels using the Confidentiality, Integrity, and Availability (CIA) model, taking into consideration the operation of OT systems
- Identify main producers of critical shipboard IT and OT equipment
- Review detailed documentation of critical OT and IT systems including their network architecture, interfaces, and interconnections
- Identify cyber security points-of-contact with each of the producers and establish a working relationship with them
- Review detailed documentation on the ship's maintenance and support of the IT and OT systems
- Establish contractual requirements and obligations that the shipowner/ship operator may have for maintenance and support of shipboard networks and equipment
- Support the risk assessment with an external expert to develop detailed plans, including producers and service providers as necessary

The goal of these assessments was to analyse and assess the ship's network, its systems/devices to identify any vulnerabilities that could compromise or result in either loss of confidentiality, loss of integrity, or result in a loss of operation of the equipment, system, network, or even the ship. These vulnerabilities and weaknesses could fall into one of the following categories:

- Technical – software defects, End of Life (EoL) or End of Support (EoS) systems
- Design – access management, unmanaged network interconnections
- Implementation – errors such as misconfigured firewall rules or access control lists
- Procedural – system and physical access or other user errors

3. Follow-on Maritime Cyber Security Implementation

After this original one-year contract, we were engaged again by one of the larger Universities in the ARF in 2024 with a Statement of Work (SOW) for Cyber Security Assessment Support to meet the new American Bureau of Shipping (ABS) Guide for Cybersecurity Implementation for the Marine and Offshore Industries (ABS CyberSafety Volume 2) dated August 2023. Peregrine conducted two Site visits to vessels in both the Pacific and Atlantic Oceans that were conducted in October – November 2024 time frame, and based upon those surveys, the Peregrine staff evaluated both vessels with CS-1 status, based on the 40 requirements per sections 1.3 of the American Bureau of Shipping (ABS) CyberSafety Vol 2, pages 26-31, as well as section 2.3 (page 34). In addition, Peregrine SMEs also reviewed with our findings with both ship's crew, to confirm that they understood and were abiding by the ABS Appendices shown below:

- Appendix 1 Maritime Cybersecurity Risk Assessment
- Appendix 2 Functional Description Document (FDD)
- Appendix 3 Cybersecurity Risk Management System (CRMS)

In addition, since Peregrine is a sponsor of the Maritime Transportation System (MTS) Security Operations Center (SOC) since 2019, https://www.mtsisac.org/, we gave for this effort the University access to all Maritime cybersecurity threats from this Department of Homeland Security (DHS) sponsored Information Sharing and Analysis Center (ISAC).

For Peregrine's most recent cyber assessments, we based it on a number of references to include:

- The Guidelines on Cyber Security Onboard Ships, version 4 published 23 December 2020 (hereafter referred to as the Baltic and International Maritime Council (BIMCO) document)
- MSC-FAL.1/Circ. 3 Guidelines
- The ABS CyberSafety Volume 2) dated August 2023

Our SMEs worked with the respective ship's crew as well the Universities IT staff to finalize the files for submission to ABS. To do this, our team followed the specific guidance from the three aforementioned references, which makes clear that an approved SMS should consider cyber risk management when meeting the objectives and functional requirements. These three documents also provided guidance on maritime cyber risk management as well as high-level recommendations regarding the elements of an appropriate approach to implementing cyber risk management. This document is designed to provide the minimum measures that all companies should consider implementing to address cyber risk management in an approved SMS.

Based on The Guidelines on Cyber Security Onboard Ships, version 4 published 23 December 2020 (hereafter referred to as the BIMCO document), along with the MSC-FAL.1/Circ. 3 guidelines, and the ABS CyberSafety Volume 2) dated August 2023, these three documents would serve as the primary reference for the Peregrine SMEs to review for their latest 2024-2025 cybersecurity accreditation effort.

- Company and Vessel Cybersecurity Representative or Organization (1 August 2023) - Company to provide documentation identifying person(s) responsible for cybersecurity, the organizational location within the Company, and quality or cybersecurity certificates (e.g., International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001, International Society of Automation (ISA)/IEC 62443, or ISASecure® certifications).
- Company and Vessel Cybersecurity Policies and Procedures (1 August 2023) - Company to provide documentation detailing cybersecurity policies and implementation procedures applied to employees, suppliers, and contractors.

- Company and Vessel Cybersecurity Incident Response (IR) and Recovery Documentation describing Company and vessel cybersecurity incident response team(s), including response and recovery responsibilities, capabilities, and staffing.
- Company and Vessel OT and Related IT System Architecture - Descriptions and diagrams detailing the OT and connected IT systems architecture that are suitable for performing a physical and cybersecurity risk assessment.
- Company and Vessel OT and Related IT Risk Assessment and Management Plan - A cybersecurity risk assessment of the OT and connected IT systems architecture, and a risk management plan derived from that assessment.
- Company and Vessel Cybersecurity Risk Management System (CRMS) Design, Operating and Maintenance Procedures - CRMS functional description document (FDD) that includes a functional architecture with an inventory and descriptions of cybersecurity protective equipment; logical and procedural protections (see Appendix 3); operating and maintenance procedures; cybersecurity event/incident corrective/ preventive action procedures; auditing and test procedures; and, change management procedures.
- Company and Vessel Cybersecurity Training Program - Documentation detailing cybersecurity training records and training content concerning cyber hygiene and support of specialized cybersecurity functions.
- Company and Vessel OT/IT Management of Change (MOC) Procedures - Documentation detailing change management and configuration control policies and procedures applied during vessel operation, including OT, OT-connected IT, and CRMS software and computer hardware registries

4. Recommendations Moving Forward

Here are some specific suggestions from the Peregrine staff based on our interviews in the 2020-2021 and 2024-2025 timeframe efforts, for any organizations that are looking to increase their cybersecurity capabilities:

- MTSC-ISAC Membership plus attend annual MTS conference
- Cybersecurity Maturity Model Certification (CMMC) Level 2.0 compliance at each University
- Updated Researcher Cybersecurity CMMC checklist for DoD Projects
- Detailed SOP between each ship and it's University IT shop
- Develop ship specific Cyber Security Response Plans and test them
- Conduct tabletop ICS cybersecurity events for both ships and WHOI IS
- North American Treaty Organization (NATO) Science and Technology Organization (STO) Centre for Maritime Research and Experimentation (CMRE). This is a world-class scientific research and experimentation facility located in La Spezia, Italy. It is an executive body of the NATO Science and Technology Organization (STO) and focuses on the maritime domain to address the defense and security needs of the Alliance. CMRE conducts scientific research and technology development in various areas, including ocean science, modeling and simulation, acoustics, and more. The facility operates two research vessels, the NATO Research Vessel Alliance and the Coastal Research Vessel Leonardo, which are used for conducting NATO research and supporting commercial or government organizations within NATO nations.

Peregrine is already a member of these organizations, and if desired, we can brief these organizations on a regular basis on any critical issues, as the MTSC-ISAC promotes and facilitates maritime cybersecurity information sharing, awareness, training, and collaboration efforts between private and public sector stakeholders. If desired, our team can also monitor and review all of the updates in requirements/mandates that would need to abide by from wrt a cyber incident, as shown in Section 3.4. Peregrine will also support the upgrade to Safety Management System (SMM) section 7.10 - regarding Cyber Risk Management which will need to be updated / revised for inclusion in our manual. Revision / update of our SMM policy, US Coast Guard Vessel Security Plans, Cyber Security Incident Plans or other shipboard procedures to adhere to current UNOLS / NSF standards.

For the 2024-2025 effort, the Peregrine SMEs in conjunction with the University staff developed the specific documents to ensure from a Safety Management System (SMS) requirements, that they had a section for Cyber Risk Management (CRM) Instructions to employ heightened awareness and to establish procedures to respond to this situation on the vessels that they operate. This is a required document, from a safety aspect and will need to be updated in 2025 to match the new ABS Cyber Survey and USCG cybersecurity regulations.

Moving forward on the Cyber Security (CS) CS-1 notation, the Peregrine SMEs finalized documentation submissions (Subsection 1/7) are to be provided for surveys of notation requirements detailed in Section 2/Tables 3 and 4, respectively. As these initial surveys were conducted in October 2024 before the final draft of the new US Coast Guard cybersecurity mandate, our SMEs went on board to confirm that the following are documented and implementation-verified moving forward:

- Vessel cybersecurity risk management system (CRMS) (Appendix 3)
- Processes and programs detailed in Section 2/Tables 3 and 4, as applicable
- Maintenance procedures supporting Company-required maintenance of OT systems, IT systems, and CRMS protections as detailed on original equipment manufacturer (OEM solution provider documentation
- Vessel-specific cybersecurity programs and capabilities including Functional Design Document description (Appendix 2) and CS-1 Requirements listed in Section 2/Table 3
- The Peregrine SMEs icw WHOI are also determining which cyber risk management systems that have been surveyed to the satisfaction of the attending Surveyor to the full requirements of this Guide as applicable, where approved by the Committee, may be classed and distinguished in the ABS Record by the notation CS-1.

Here are the specific CS-1 Submittals that we complied with for this latest cyber assessment:

- Company and Vessel Cybersecurity Representative or Organization (1 August 2023) Company to provide documentation identifying person(s) responsible for cybersecurity, the organizational location within the Company, and quality or cybersecurity certificates (e.g., ISO/IEC 27001, ISA/IEC 62443, or ISASecure® certifications).
- Company and Vessel Cybersecurity Policies and Procedures (1 August 2023) Company to provide documentation detailing cybersecurity policies and implementation procedures applied to employees, suppliers, and contractors.
- Company and Vessel Cybersecurity Incident Response (IR) and Recovery. Documentation describing Company and vessel cybersecurity incident response team(s), including response and recovery responsibilities, capabilities, and staffing.
- Company and Vessel OT and Related IT System Architecture. Descriptions and diagrams detailing the OT and connected IT systems architecture that are suitable for performing a physical and cybersecurity risk assessment.
- Company and Vessel OT and Related IT Risk Assessment and Management Plan. A cybersecurity risk assessment of the OT and connected IT systems architecture, and a risk management plan derived from that assessment.
- Company and Vessel Cybersecurity Risk Management System (CRMS) Design. Operating and Maintenance Procedures CRMS functional description document (FDD) that includes a functional architecture with an inventory and descriptions of cybersecurity protective equipment; logical and procedural protections (see Appendix 3); operating and maintenance procedures; cybersecurity event/incident corrective/ preventive action procedures; auditing and test procedures; and, change management procedures.
- Company and Vessel Cybersecurity Training Program. Documentation detailing cybersecurity training records and training content concerning cyber hygiene and support of specialized cybersecurity functions.
- Company and Vessel OT/IT Management of Change (MOC) Procedures. Documentation detailing change management and configuration control policies and procedures applied during vessel operation, including OT, OT-connected IT, and CRMS software and computer hardware registries

From the new USCG Cybersecurity regulation, there are three main parts, specifically to maintain a Cybersecurity Plan, to designate a Cybersecurity Officer (CySO) and to implement a Cyber Incident Response Plan as part of the annual audit. Here are specific requirements:

- Cybersecurity Plan (101.630) with seven account security measures, plus four security measure requirements as well as two data security measure requirements
- Designate a Cybersecurity Officer to implement the Cybersecurity Plan and the Cyber Incident Response Plan, plus lead the annual audit as well as cybersecurity inspections. The CYSO must be accessible to the USCG 24/7.
- Drills and exercises (101.635) – at least once a year

- Records and Documentation (101.640) – for at least 2 years
- Specific Cybersecurity Measures (101.650) – sections a through I, covering all security measures, training, risk management, supply chain and physical security
- It also references the need for a Cyber Incident Response Plan

Peregrine as part of its future support has already started to draft the Cybersecurity Plan using this format:

- Cybersecurity Organization / CySO
- Personnel Training
- Drills and Exercises
- Records and Documentation
- Communications
- Cybersecurity Measures/Routine Maintenace
- Cybersecurity Measures/Account Measures
- Cybersecurity Measures/Physical Security
- Cybersecurity Measures/Supply Chain
- Cybersecurity Plan/Audits
- Cybersecurity Measures: Risk Management (Reports)
- Cybersecurity Measures: Risk Management (Vulnerabilities)
- Cybersecurity Measures: Resilience
- Cybersecurity Measures: Risk Management (Assessment)

As noted, the Peregrine SMEs have also drafted proposed cybersecurity playbooks for the following Cyber Incident Response Plan:

- Compromised Navigation System
- Malicious Software
- Loss of Internet
- Ransomware
- Phishing

Finally, we noted that the there are other entities that are striving to make strategic and appropriately aggressive decisions to incentivize industry adoption, improve productivity, and appropriately balance risks and opportunities. One area of expertise from Peregrine perspective that we can help WHOI to focus on more is cybersecurity for industrial control systems, and our SMEs can ensure that that these additional requirements are met moving forward to comply with these requirements:

- Maritime Cyber Risk Management in Safety Management Systems (MSC-FAL.1/Circ. 3)
- Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Mgmt Systems
- National Cybersecurity Center of Excellence - Securing Water and Wastewater Utilities Sector and Chemical Companies to outline cybersecurity posture at OT / ICS threats plus Responding /Recovering from cybersecurity incidents within the Manufacturing Sector
- NIST SP 800-160 - Revised guidance on engineering trustworthy secure systems
- Government Accountability Office (GAO) - Reports offshore oil and gas infrastructure faces cyber risks
- DHS - Testing environments to safeguard transportation infrastructure

5. Conclusion

Over the last decade, Peregrine has been collaborating from a mission-based aspect to lock down ICS using cyber risk assessments, plus we have developed a TTX that utilizes five playbooks of possible scenarios:

- Compromised Navigation System
- Malicious Software
- Loss of Internet
- Ransomware
- Phishing

We believe that taken together, this approach will facilitate the norming of best practices/processes and risk frameworks for cyber vulnerabilities on common OT platforms/components beyond the scope of traditional Information Security. Taken together, Peregrine has developed a holistic ICS /OT cybersecurity training regime

for the maritime environment that can be utilised in a number of unclassified as well as military / commercial environments, and we have the staff available to support any entities as needed.

Ethics Declaration: I did not need an ethical clearance for this research paper.

AI Declaration: I did not use an AI tool in the development of the paper.

References

International Maritime Organization (IMO) released a Maritime Safety Committee (MSC) resolution that addresses Maritime Cyber Risk Management in Safety Management Systems (MSC-FAL.1/Circ. 3), MSC-FAL.1-Circ.3-Rev.3.pdf

Cybersecurity Implementation for the Marine and Offshore Industries, ABS CyberSafety® Vol 2, Aug 23, Cybersecurity Implementation for the Marine and Offshore Industries

U.S. Coast Guard Issues Final Rule & Request for Comments on New Cybersecurity Regulations for the Marine Transportation System, 17 January 2025, Cyber Regulations Fact Sheet for Public Release_CLEAN_15JAN2025.pdf

The Guidelines on Cyber Security Onboard Ships, BIMCO, 4 January 2021, The Guidelines on Cyber Security Onboard Ships