GUIDE FOR

CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES

ABS CyberSafety™ VOLUME 2

SEPTEMBER 2016 (Updated 15 June 2018 – see next page)

American Bureau of Shipping
Incorporated by Act of Legislature of
the State of New York 1862

ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA

Updates

15 June 2018 consolidation includes:

- 1 June 2018 version plus Notice No. 2

June 2018 consolidation includes:

- September 2016 version plus Notice No. 1

Foreword *(15 June 2018)*

In the maritime world, safety and security are closely linked. The mission of ABS is to serve the public interest as well as the needs of our members and clients by promoting the security of life and property, and preserving the natural environment. For over 150 years, ABS has devoted its energies to promoting safe and efficient commerce by sea through the development and application of industry consensus standards. Initially, the emphasis was on safety, and ABS applied its technology and knowledge to maintain safety through prevention of accidents caused by the forces of nature and human error. While the science of those causes is very complex and is continually being improved, they are amenable to analysis, understanding and prediction. Through the dedication and diligence of everyone in the maritime industries, the safety record of shipping has steadily improved through the years.

Cybersecurity introduces an additional element into the safety equation: security against deliberate actions intended to cause harm. Security has always been a concern with naval ships, and the military routinely exercise precautions to maintain the security of their ships and offshore assets. Commercial vessels routinely employ special security measures under certain circumstances to prevent theft, piracy, smuggling or stowaways. Those crimes are usually economically motivated, where destruction is not the goal. Acts of terror are usually politically motivated, and ships and offshore assets are prime targets because of their mobility and high potential for causing extensive damage to life, property, the environment, and the transportation and economic infrastructure. The maritime community has come to the realization that ships and offshore assets must be made less vulnerable to security threats, both at sea and while in port. Perpetrators of such acts have moved toward cyber-attacks for similar purposes. Exposure to these threats has become pervasive due to the exponential growth of automation methods – and increasingly, autonomy – that has penetrated nearly all aspects of shipboard and offshore asset systems. Because these systems control multiple aspects of asset, ship or platform operations, they become integral parts of system and operational safety.

ABS supports the marine and offshore communities by developing the standard for marine and offshore cybersecurity, developing new methods and leading industry with best practices in a commitment to safety and security of life and property and preservation of the environment.

Cybersecurity refers to the security of information networks and control systems and the equipment and systems that communicate, store and act on data. Cybersecurity encompasses systems, ships and offshore assets, but includes third parties – subcontractors, technicians, suppliers – and external components such as sensors and analytic systems that interface with networks and data systems. This includes human interaction of crews and other Company personnel, customers and potential threat players. In such a dynamic system, cybersecurity is an evolving set of capabilities inside the Company, developing and adapting as technology and threats evolve.

Volume 1 of the ABS CyberSafety™ series provides best practices as a foundational element of overall safety and security within and across the marine and offshore communities. Cybersafety encompasses a number of elements including basic cyber systems operations, system and system of systems requirements to enhance safety as well as cyber security in the interest of enhanced safety. This document is Volume 2 of the ABS CyberSafety™ series. It provides criteria for the assessment of corporate systems and asset readiness to prevent cyber events that may compromise the safety and security of the data, systems and assets.

ABS offers the optional **CS** series (**CS1**, **CS2**, **CS3**, **and CS-Ready**) Class notation to ships and offshore assets that comply with ABS requirements contained in this Guide. The notation is available for all classed vessels complying with the IMO International Safety Management (ISM) Code. While the notation is not required as a condition for ABS Class, ABS believes that the ABS CyberSafety™ Class notation is a useful indication of the due diligence applied by owners to better prepare for cybersecurity concerns affecting ships, offshore assets and their associated shoreside facilities. The **CS-Ready** Notation is intended for newly constructed assets and is provided to the vessel based on specifically focused requirements as indicated in Section 8 of this Guide.

The maritime cybersecurity area is evolving rapidly, and the International Maritime Organization (IMO), the International Association of Classification Societies (IACS), governmental authorities, and ABS are expected to add to the resources available to prepare Owners of ships and/or offshore assets for the new security environment.

This Guide becomes effective on the first day of the month of publication.

Users are advised to check periodically on the ABS website www.eagle.org to verify that this version of this Guide is the most current.

We welcome your feedback. Comments or suggestions can be sent electronically by email to rsd@eagle.org.

GUIDE FOR

CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES

ABS CyberSafety™ VOLUME 2

CONTENTS

This Page Intentionally Left Blank

SECTION 1 Introduction to the Guide

1 General

This Guide for ABS CyberSafety™ has been developed so as to reduce cybersecurity-related conditions or incidents that may negatively affect systems, ships, offshore assets, safety, or the performance of cyber-enabled systems. ABS recognizes the positive impact that sound cybersecurity management practices have in reducing losses to the maritime industry due to unauthorized access into control systems from criminal or unintended activity. This Guide provides a model for implementing cybersecurity programs.

This Guide presents criteria for compliance with ABS CyberSafety™ requirements. These requirements will be used by ABS in the cybersecurity reviews and surveys of information technology (IT) systems; operational technology (OT) control systems; and their system interfaces and software on ships, offshore assets and the management systems of the associated shoreside facilities.

This Guide emphasizes implementation and verification of organizational processes and business rules (i.e., controls) through review and audit methods, and technical verification of system protective mechanisms and technical controls through system testing.

Criteria for the hardware and software integrity of computer-based control systems are given in other ABS Rules and Guides, such as the ABS *Rules for Building and Classing Steel Vessels (Steel Vessel Rules)*, the ABS *Guidance Notes on Failure Mode and Effects Analysis (FMEA) for Classification*, the ABS *Guide for Integrated Software Quality Management (ISQM)*, and other applicable national and international standards.

3 Application and Scope *(15 June 2018)*

3.1 Application

This Guide is intended for use by companies operating all types of ships and offshore assets. Additionally, the Guide intended for use by companies (i.e., Shipbuilders and Integrators) constructing those assets. The Guide's requirements are stated in general terms in order to apply to a wide variety of ships and offshore assets and their operating Companies.

The term "ships" includes passenger ships, cargo ships, mobile offshore units, and high speed craft. This Guide may also be used for fixed or floating offshore production assets. If requested by the owner, ABS will verify and certify the Cybersecurity program of any ship or vessel and its associated shoreside facilities in accordance with this Guide.

In general, this Guide is intended to apply to vessels and their operating Company. A vessel may be certified without certifying the Company or its facilities so long as appropriate boundaries are defined and verified in accordance with this Guide.

3.3 Scope

The requirements herein are applicable to standalone or integrated computer-based information technology and operational technology systems. Such systems may be installed on a ship, offshore unit, or land based Company facilities.

Compliance with the procedures and criteria given in this Guide may result in issuance of a:

- CyberSafety Management System Certificate (CMSC) or Notation **CS1**, **CS2**, **CS3**, to an ABS classed ship or offshore asset upon request. Ships and offshore assets not classed by ABS can be issued a "Statement of Fact" when they are in conformance with the requirements of this Guide.
- Certificate of Cyber Compliance (CCC) for the Company's examined Facility or vessel under construction.

The intent of the **CS** Notation series is to define boundaries of critical systems in the shipboard networked environment. Primary Essential Services, as defined by Integrity Levels and criticality to human, asset or environmental safety, are to be protected for a vessel or unit to be eligible for the **CS** notation, within the defined system boundaries. Primary Essential Services are defined in 4-8-1/Table 1 of the *Steel Vessel Rules* or 4-1-1/Table 3 of the *MODU Rules*.

Operational Technology (OT) in Primary Essential Services, including process and systems control hardware and software, is addressed in ABS CyberSafety™ with the intent that control systems are built and operated in known conditions; that without operator alerts they cannot be accidentally or malevolently affected in ways that impact human, system or environmental safety; and that OT is sustained and maintained across its lifecycle with proper care and diligent attention to keep both controls and their systems safe.

Additional functions of the connected equipment are not included in the Notation unless detailed in the verification plan.

5 Certification

5.1 General *(1 June 2018)*

Companies seeking certification to this Guide must, as a condition of certification, conform to the requirements of the ISM Code as relevant to the selected scope of their organizational management system.

The scope of certification chosen by the Company may include vessels, offshore assets, and/or the Company's facilities in combination(s) chosen by the Company. Vessel selection considers all vessels in the fleet but centers on the vessels considered highest priority by the Company. At least one vessel of each selected type is to be presented as a sample to be maintained at certification within the same scope of certification as required by the Company. The Company must provide evidence of verifiable similarity[1] among ships and offshore assets of specific types if any survey or test operations are to be abbreviated on the basis of identical installations or commonality across ships and offshore assets.

Ships and offshore assets certified to the requirements of this Guide are, as a prerequisite, to be Classed by ABS or another International Association of Classification Societies (IACS) member to confirm CyberSafety builds on existing safe, monitored and managed assets. In the case of critical equipment or systems requested for specific review under the terms of this Guide, those systems must be Classed by ABS or another IACS member prior to consideration, for the same reasons as for ships and offshore assets Class requirements.

Vessels shall be assessed on an annual basis, when there are major cyber-enabled, safety-related networked system configuration changes[2], or with multi-year Class survey events when no major system configurations are changed. Annual Surveys are to be made within three months before or after each anniversary date of the crediting of the previous Special Periodical Survey or original construction date. Surveys/Audits for Certification to this Guide will be harmonized with extant ABS Classification, Statutory and HQSE-En survey/audit cycles to the extent possible.

A Company's Facility that is assessed by ABS and found to meet the requirements specified in this Guide may be issued a corresponding Certificate of CyberSafety Compliance (CCC). Vessels operating under the Company's Cybersecurity Management System that are assessed by ABS and found to meet the requirements specified in this Guide may be issued a CyberSafety Management System Certificate (CMSC) as findings of the assessment[3]. The Notations and their meanings are listed below in Subsection 1/7.

All certificates are subject to periodic and intermediate verifications conducted at each certified location. All certifications are nontransferable. Assessments are based upon a sampling process. The absence of recorded nonconformities does not mean that none exist. Nothing contained herein or in any certificate, notation, or report issued in connection with a certificate and/or notation is intended to relieve any designer, builder,

[1] Similarity includes not just type design (unit 1, unit 2, of a series), but also similarity of control system construction and implementation. Programmable Logic Controllers (PLCs) used in specific systems must be shown as sufficiently similar across units with a ship type that understanding of control systems is possible through documentation of those systems.

[2] Examples of changes sufficient to force reassessment of cyber-enabled, safety-related networked systems include major-version-number operating system or firmware changes in either OT or IT; control system changeouts in safety-critical systems; or combined configuration changes between or among two or more systems that control safety-critical systems. Other examples also apply.

[3] As stated in 1/3.3, non-ABS-classed vessels will be issued a Statement of Fact in place of the CMSC or Notation.

owner, manufacturer, seller, supplier, repairer, operator, insurer, or other entity of any duty to inspect or any other duty or warranty, express or implied, nor to create any interest, right, claim, or benefit in any insurer or other third party.

This Guide is subject to review and revision. Updates may include, among other things, additional requirements, or clarification of existing requirements. All Guide related modifications need to meet the latest version of the Guide and major changes may require the entire system be recertified to the latest version of the Guide. Survey requirements are to be carried out to the latest Guide, and we reserve the right to make any changes or updates retroactive.

5.3 Certification Process *(1 June 2018)*

Companies seeking certification to the requirements of this Guide shall fulfill the following responsibilities, some of which are more fully described in subsequent sections of the Guide:

i) Document, implement, and maintain a cybersecurity management system in accordance with the pertinent requirements of this Guide.

ii) Provide ABS copies of Cybersecurity Management System documentation for review, in accordance with the requirements of this Guide.

iii) Allow ABS access to all certified locations and vessels during appropriately scheduled working hours so as to assess the Cybersecurity Management System and relevant systems (information technology (IT), operational technology (OT), or both, including data infrastructure and interface systems) to determine continuing compliance with the pertinent requirements of this Guide.

iv) Maintain a log or compiled record of all modifications, maintenance and system security or configuration updates and upgrades, including any outstanding help desk tickets or vendor/integrator repair or maintenance requirements, and any insecurities or breaches, and the resolution thereof[4].

v) Notify ABS of port state detentions of vessel(s). In the case of cyber-enabled, safety-related system assessments, inspections or audits that result in unsatisfactory port state findings concerning systems included in the verification plan for this Notation, note to ABS the details of the same.

vi) Inform ABS in writing when an ISM Document of Compliance (DOC) or Safety Management Certificate is withdrawn or invalidated by the issuing party for vessels certified to the requirements herein.

vii) Submit plans and data as documented in Subsection 1/15.

viii) Inform ABS in writing of major changes to organizational management system elements (e.g., managerial organizational structure, location, change in types of vessels operated, upgrade/downgrade of process capability, control, or flow) so that the changes may be evaluated by ABS and appropriate action taken.

5.5 Survey and Certification Process *(1 June 2018)*

i) ABS CyberSafety™ certification is an annual process for ships and/or facilities that seek to achieve and maintain the Notation and/or certificate. Survey for ABS CyberSafety™ certification includes the factors listed in 1/5.3 above, emphasizing documentation, operational cybersecurity management system viability, strict control of configurations and changes in networked or cyber-enabled assets, and organizational capabilities in place and functioning. ABS will provide detailed checklists to the owner, supplementing the capability specifications in Section 5, for progress checking and current-status documentation.

ii) Periodicity for ABS CyberSafety™ certifications will harmonize with standard ABS Survey requirements, and ABS will coordinate surveys and evidence-based assessments wherever possible.

[4] This log is to be in a digital, searchable form. Non-searchable images of system, ship or asset operational manuals in documentation packages extend the duration and difficulty of survey and assessment. Proprietary documentation will remain with the owner, builder, operator, etc. if so specified or desired.

a) *Surveys During Construction.* ABS Engineering and Survey personnel assigned to a newbuild project will actively collaborate to check design such that safety principles are integrated, and that ABS CyberSafety™ assessments and survey(s) are conducted in consonance with conventional survey events.

b) *Surveys After Construction.* The Annual Surveys should coincide with the Class Periodical Surveys. These will be supplemented by ABS CyberSafety™ assessments as required. Annual recertification includes the documentation required in 1/5.3 above, given the fluid nature of information and automation technologies.

c) *Special Surveys.* ABS CyberSafety™ surveys and assessments may be required after equipment or control system changes (major system changes or configuration changes), after security events occur, or on an as-required basis from the Company.

d) Certification will expire at the end of the stated period on the CCC or CMSC. Recertification, assuming documentation is provided (as in 1/5.3 above) and reassessment or testing is completed in a timely fashion, is expected to be a shorter and more streamlined evolution than initial certification.

iii) *Relationship between Survey (or Continuous Survey) and ABS CyberSafety™ Certification.* Class, as maintained through regular Surveys or through Continuous Survey, reviews overall technical and procedural compliance for requirements in accordance with the overarching Steel Vessel Rules, outside the ABS CyberSafety™ certification. Class, especially in conditions of Continuous Survey, includes ABS CyberSafety™ certification when requested, though said certification is a snapshot in time within the Class continuum.

5.7 Representations

Certification is a representation by ABS that at the time of assessment the Company and vessels, as pertinent, has established and implemented a Cybersecurity Management System in accordance with the requirements in this Guide for the specified certificates and notations, and that the assessments, inspections, tests and audits for appropriate security profiles and risk conditions were completed satisfactorily. Certification is not a representation that the Company always acts in compliance with the cybersecurity program or that the cybersecurity program addresses all contingencies. Management performance remains the responsibility of the Company.

5.9 Termination

The continuance of certification or any notation is conditional upon the Company's and vessels' continued compliance with the pertinent requirements of this Guide. ABS reserves the right to reconsider, withhold, suspend, or cancel the certification or Notation for noncompliance with the Notation requirements, refusing access to a vessel, unit, or facility for an assessment or verification, or nonpayment of fees which are due on account of certification and other services.

Upon change of vessel or asset ownership, or of management organization, ABS reserves the right to perform out-of-cycle reassessments to check that the Notation remains current under the new organization. The essence of this Guide is building, maintaining and sustaining enabling capabilities for security and safety of cyber-enabled systems; a change in ownership or management will necessarily indicate a change in Company capability to support secure and effective operations in vessel or asset systems.

5.11 Limitation of Liability

ABS shall not be liable or responsible in any respect for any inaccuracy or omission in this Guide or any other publication or document issued by ABS related to this Guide. Every owner, builder, or operator must understand their systems in order to tailor the application of security controls and requirements, filling gaps in their security where needed by specific situations. This Guide is not meant to address every possible contingency, but rather provide a means by which owner/builder/operator may execute a security program that may, in operations, reveal needs for tailored or unique security controls.

7 Notation *(15 June 2018)*

The **CS** Notation will be assigned upon achieving compliance with the procedures and criteria given in this Guide for cybersecurity implementation and subsequent verification. Maintenance of the **CS** notation over the operational life of the vessel, platform, facility or asset is subject to continued compliance as evidenced by satisfactory completion of periodic surveys conducted onboard the vessel, or at the asset or facility. The intent of the Notation is to define boundaries of safety-critical systems in the shipboard or platform networked environment, (i.e., ABS CyberSafety™ verification will address systems critical to human, vessel, platform, system or environmental safety and will be detailed in a verification plan). Non-safety-related connected control systems or information systems and non-safety-related functions of the connected equipment are not included in the Notation unless detailed in the verification plan. The **CS** notation may be assigned as follows:

CS1 Informed Cybersecurity Implementation

CS2 Rigorous Cybersecurity Implementation

CS3 Adaptive Cybersecurity Implementation (Highest level of Readiness)

CS1, **CS2**, or **CS3** are more fully described in Section 3 of this Guide. The **CS** notation will be made available to the owner via the ABS *Record* in a protected form enabling disclosure by the owner only to parties with a need to know[5].

Control systems within the scope of the **CS** notation will be listed in the ABS *Record* to describe the exact coverage of the notation. For example, the descriptor could be one or more of the following:

- Vessel Management Control System
- Power Management Control System
- Dynamic Positioning Control System
- Drilling Control System
- etc.

The **CS** Notation may itself be annotated in the case of a Company that certifies a facility or facilities in addition to vessel(s). The Notation would thereby reflect as **CS1+**, **CS2+**, or **CS3+**. This is expected in cases of advanced vessels that will link control systems between vessel and onload/offload facility to regulate cargo or hazardous operations through cyber-enabled systems.

A **CS-Ready** Notation is also available for the Owner/Operator if the SBI constructs a vessel based on the requirements in Section 8 of this Guide. The Notation would read **CS-Ready**.

9 Organizations

9.1 Company

The Company is the Organization that initiates the project and owns the information system and/or control system at the end of the project.

9.3 Ship Builder Integrator (SBI)

For new builds, the SBI is the shipyard. If no shipyard is involved, then the activities and requirements listed for the SBI are to be performed by the Owner.

9.5 System Provider (SP)

System Providers (SP) are suppliers that developed the software for the system under software verification test subject to system verification. If multiple systems are selected for system verification, then there may be multiple SPs. This may also include Original Equipment Manufacturer (OEM) for majority of hardware systems.

[5] An expanded notation of **CS1+**, **CS2+**, or **CS3+**, as noted in Section 3, addresses ship and Company facility.

9.7 Sub-Supplier (Component Providers)

A sub-supplier is a supplier of connected equipment to the SP's control system and subject to integration portion of the verification testing.

11 Definitions *(15 June 2018)*

The definitions listed below are taken, or adapted from the ISM Code, ISO 9001:2015, ISO 14001:2015, ISO 50001:2011, and OHSAS 18001:2007.

ABS CyberSafety™. Guidelines and standards for computerized, automated, and autonomous systems that provide confidence that those systems are designed, built, operated, and maintained so as to allow only predictable, repeatable behaviors.

Acceptable Risk. Risk that can be tolerated by the Company having regard to its legal obligations and its own OH&S policy.

Administration. The Government of the State whose flag the ship is entitled to fly.

Anniversary Date. The day and month of each year that corresponds to the date of expiry of the relevant document or certificate.

Audit. Systematic, independent, and documented process for obtaining "audit evidence" and evaluating it objectively to determine the extent to which "audit criteria" are fulfilled.

Auditor. Person with the competence to conduct an audit.

Boundaries. Physical or site limits and/or organizational limits defined by the Company. (ISO50001:2011)

CCC. A Certificate of Cyber Compliance, which may be issued to a Company that is assessed by ABS and found to meet the requirements specified in this Guide.

CMSC. Vessels not requesting CyberSafety™ notations, operating under the Company's cybersecurity management system, that are assessed by ABS and found to meet the requirements specified in this Guide may be issued a Cyber Safety Certificate (CMSC), containing findings of the assessment.

Capability. The ability to execute a specified course of action.

Certification. Confirmation decision by ABS that the Company's management system meets the applicable requirements of this ABS Guide.

Company. The Owner of the ship or any other organization or person, such as the manager or the bareboat charterer, who has assumed the responsibility for operation of the ship from the ship owner and who, on assuming such responsibility, has agreed to take over all duties and responsibilities imposed by the ISM Code and this Guide; Organization [ISO 9001:2015, ISO 14001:2015, ISO 50001:2011, and OHSAS 18001:2007]. For Government-owned vessels in non-commercial service, the Naval Administration is to be considered the Company.

Company Information Security Officer (CISO). The individual responsible for information systems, control systems and data security within the Company's enterprise.

Continual Improvement. Recurring process of enhancing the management system in order to achieve improvements in overall performance.

Control System. Set of devices that manages, commands, directs or regulates the behavior of other devices or systems according to user inputs, settings or configurations.

Correction. Action to eliminate a detected non-conformity.

Corrective Action. Action to eliminate the cause of a detected nonconformity or other undesirable situation.

CS-Ready. Indicates the hardware and systems of the vessel are built, integrated and documented in accordance with appropriate Cybersecurity practices outlined in Section 8 of this Guide.

Cyber-Enabled System. Computerized or programmable system built to provide significant degrees of automation in operational function, system monitoring and management, or data communications.

Cybersecurity Management System. An organizational tool for the identification, prioritization, execution and monitoring of the Company's cybersecurity policies, processes and procedures

CyberSafety Management System Certificate (CMSC). Certificate of compliance provided for a vessel's successful assessment of capabilities and practices required for CyberSafety under this Guide.

DOC. ISM Document of Compliance certificate

Document. Information and its supporting medium.

Documentation. Records and certificates that confirm that the ship is in compliance with applicable security requirements.

Energy. Electricity, fuels, steam, heat, compressed air, and other like media.

Environment. Surroundings in which a Company and its ships or offshore assets operate, including air, water, land, natural resources, flora, fauna, humans, and their interrelation.

Environmental Aspect. Element of a Company's activities or products or services that can interact with the environment.

Environmental Impact. Any change to the environment, whether adverse or beneficial, wholly or partially resulting from a Company's environmental aspects.

Environmental Objective. Overall environmental goal, consistent with the environmental policy, that a Company sets itself to achieve, and which is quantifiable where practicable.

Environmental Management System. Part of a Company's management system used to develop and implement its environmental policy and manage its environmental aspects

Environmental Performance. Measurable results of a Company's management of its environmental aspects.

Environmental Target. Detailed performance requirement that arises from the environmental objectives

Executive Management. Person(s) who directs or controls a Company at the highest level.

FDD – Functional Description Document. Revision-controlled document containing a description of the industrial control system (ICS) equipment and control systems in a form readily understandable by shipboard personnel who are (a) technically competent in shipboard operations, and are (b) authorized to evaluate, operate, or maintain those equipment and control systems.

Hazard. Source, situation or act with a potential for harm, in terms of injury or ill health, damage to property, damage to workplace environment or a combination of these.

Hazard Identification. Process of recognizing that a hazard exists and defining its characteristics.

ICS – Industrial Control System. Control system for industrial or machinery processes.

Information System. Automated system that enables Company and use of data.

Information Technology. Automated systems used for storing, retrieving, processing and sending data.

Infrastructure. System of facilities, equipment, and services needed for the operation of the Company.

Incident. Work-related event(s) in which an injury or ill health (regardless of severity) or fatality occurred or could have occurred.

Integrity Level. Assessment grade for the importance of a system to safety or operations, based on the consequences of failure of the function, component or system; represents how important the function is to the operation of the overall system.

Internal Audit. Systematic, independent, and documented process for obtaining evidence and evaluating it objectively to determine the extent to which the management system audit criteria set by the Company are fulfilled

Interested Parties. Person or group, inside or outside the workplace, concerned with or affected by the performance of the Company.

ISM. International Management Code for the Safe Operation of Ships and for Pollution Prevention as adopted by the formal body that determines these safety rules.

Major Non-conformity. The deviation that poses a serious threat to the safety of personnel or the ship or a serious risk to the environment that requires immediate corrective action or the lack of effective and systematic implementation of the requirement of the Code.

Mission-Critical System. A cyber-enabled component or system installed in a ship, facility, mission system or asset (e.g., offshore platform) that is required to carry out functions necessary to the business purposes of the system or asset, and without which the ship, facility, mission system or asset would be greatly hindered.

Non-conformity. An observed situation where objective evidence indicates the non-fulfillment of a specified requirement.

Notation. Documentation in the ABS *Record* upon certification to recognize that the ABS classed vessel meets the applicable requirements of this Guide.

Objective. A goal stated in terms of the management system's performance, that the Company sets itself to achieve.

Objective Evidence. Quantitative or qualitative information, records, or statements of fact pertaining to safety or to the existence and implementation of a safety management system element, which is based on observation, measurement, or testing that can be verified.

Observation. Statement of fact made during a management audit and substantiated by objective evidence.

Occupational health and safety (OH&S) – conditions and factors that affect, or could affect, the health and safety of employees, temporary workers, contractor personnel, visitors, and any other person in the workplace.

OH&S Management System. Part of the Company's management system used to develop and implement its OH&S policy and manage its OH&S risks

Operational Technology. Automated systems, including hardware and software, that performs direct monitoring and/or control of physical devices, processes or events; superset of industrial control systems.

Performance. Measurable results of the Company's management of its impacts and/or risks and achievement of its objectives.

Policy. Overall intentions and direction of a Company related to its performance as formally expressed by the top management.

Preventive Action. An act to eliminate the cause of a potential non-conformity or other undesirable potential situations.

Prevention of Pollution. Use of processes, practices, techniques, materials, products, services, or energy to avoid, reduce, or control (separately or in combination) the creation, emission, or discharge of any type of pollutant or waste in order to reduce adverse environmental impacts.

Procedure. Specified way to carry out an activity or a process.

Record. Document stating results achieved or providing evidence of activities performed.

Remote Access. A method of gaining access to distant assets through network connections; may refer to personnel access to network resources, such as through Virtual Private Network (VPN), or it may refer instead to direct connection to control systems equipment by connection utilities such as secure shell (SSH).

Requirement. A need or expectation stated, implied or obligatory

Risk. Combination of the likelihood of an occurrence of a hazardous event or exposure(s) and the severity of injury, ill health, or system or environmental impact that can be caused by the event or exposure(s).

Risk Assessment. Overall process of evaluating the risk(s), arising from a hazard(s), taking into account the adequacy of any existing controls, and deciding whether or not the risk(s) is acceptable.

Safety Aspect. Element of a Company's activities or services that represents an actual or potential risk to safety or personnel, or the ship, relating directly to the Integrity Level of a given system and its criticality to overall human and system safety.

Safety-Critical System. A cyber-enabled component or system installed in a ship, facility, mission system or asset (e.g., offshore platform) that is required to carry out mission-critical functions, and which, through failure or incomplete operation, may cause safety impacts to personnel, to the ship or asset, or to the environment.

Ship Security Assessment (SSA). A risk based analysis of security-related hazards or threats for each ship the Company operates.

Ship Security Officer (SSO). The individual on board each ship who is responsible for ensuring that the SSP is implemented at all times while the ship is underway and in port. The SSO also is responsible for ensuring that the SSP is maintained up-to-date and that the ship's crew are trained and familiar with their security related duties.

Ship Security Plan (SSP). A ship-specific document based on the SSA that identifies equipment, measures and procedures that are to be employed to maintain security on board the ship.

Significant Energy Use. Energy use accounting for substantial energy consumption and/or offering considerable potential for energy performance improvement.

SMC. ISM Safety Management Certificate.

SOLAS Convention. Means the International Convention for Safety of Life at Sea, 1974, as amended.

Supplier. Company or person that provides a product or service.

System. A set of interrelated or interacting elements required to direct and control a Company.

Two-factor authentication. Means of gaining access to resources with both personal login identifier and a technical factor (such as a changing-key fob or a mobile phone keycode) that confirms the identity of the user logging into the resource, and which helps to prevent illicit access by credential theft alone.

Work Environment. Set of conditions or physical location, under control of the Company, in which the work and related activities are performed.

In this document, text that appears in italics is taken directly from the cited standard. Text in standard font comprises the ABS recommendations and requirements.

13 References

13.1 ABS

ABS *Rules for Building and Classing Steel Vessels*

ABS *Guidance Notes on Application of Cybersecurity Principles to Marine and Offshore Operations – ABS CyberSafety™ Volume 1*

ABS *Guidance Notes on Data Integrity for Marine and Offshore Operations – ABS CyberSafety™ Volume 3*

ABS *Guide for Software Systems Verification – ABS CyberSafety™ Volume 4*

ABS *Guidance Notes on Software Provider Conformity Program – ABS CyberSafety™ Volume 5*

ABS *Guide for Dynamic Positioning Systems*

ABS *Guide for Integrated Software Quality Management (ISQM)*

ABS *Guide for Risk Evaluations for the Classification of Marine Related Facilities*

ABS *Guide for Survey Based on Reliability Centered Maintenance*

ABS *Guide for Surveys Using Risk-Based Inspection for the Offshore Industry*

ABS *Guidance Notes on Reliability-Centered Maintenance*

ABS *Guidance Notes on Risk Assessment Application for the Marine and Offshore Oil and Gas Industries*

ABS *Guidance Notes on Failure Mode and Effects Analysis (FMEA) for Classification*

ABS *Guide for Surveys Based on Machinery Reliability and Maintenance Techniques*

13.3 IEEE

IEEE Std 14764-2006, Second edition 2006-09-01, Software Engineering – Software Life Cycle Processes – Maintenance

IEEE Std 12207-2008, Second edition, 2008-02-01, Systems and software engineering – Software life cycle processes

IEEE Std 730-2002, IEEE Standard for Software Quality Assurance Plans

IEEE Std 1012-2004, IEEE Standard for Software Verification and Validation

IEEE Std 1016-1998, IEEE Recommended Practice for Software Design Descriptions

IEEE Std 1219-1998, IEEE Standard for Software Maintenance

IEEE Std 1362-1998 (R2007), IEEE Guide for Information Technology – System Definition – Concept of Operations (ConOps) Document

IEEE SWEBOK 2004, Software Engineering Body of Knowledge

13.5 IEC

IEC 61508-0 (2005-01), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508

IEC 61508-1 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements

IEC 61508-2 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

IEC 61508-3 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements

IEC 61508-4 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations

IEC 61508-5 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels

IEC 61508-6 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

IEC 61508-7 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures

IEC 61511-1 (2003-01), Functional safety – Safety instrumented systems for the process industry sector, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements

IEC 61511-2 (2003-07), Functional safety – Safety instrumented systems for the process industry sector, Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1

IEC 61511-3 (2003-03), Functional safety – Safety instrumented systems for the process industry sector, Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels

IEC 62351 (Power systems management and associated information exchange - Data and communications security)

ISA/IEC 62443 (Industrial Automation and Control Systems Security) Standard of Good Practice for Information Security (Published by the Information Security Forum (ISF))

13.7 ISO

ISO 17894-2005 General principles for the development and use of programmable electronic systems in marine applications

ISO/IEC 9126-1:2001 Software engineering – Product quality – Part 1: Quality model

ISO 9001:2015, Quality Management Systems – Requirements

ISO/IEC 20000-1:2011 Information Technology – Service Management - Part 1: Service management system requirements

ISO/IEC 27001:2013 - Information Technology - Security techniques - Information security management systems – Requirements

ISO/IEC 27002:2013 - - Information Technology - Security techniques - Code of practice for information security controls

ISO 28001:2007 - Security management systems for the supply chain; Best practices for implementing supply chain security, assessments and plans - Requirements and guidance

ISO 31000:2009 – Risk management – Principles and guidelines

13.9 Other

ANSI/ISA-84.00.01-2004, Part 2 (IEC 61511-2 Mod) Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) – Informative

National Institute for Science and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Feb 2014.

Software Engineering Institute. The Capability Maturity Model: Guidelines for Improving the Software Process, Reading, MA, Addison-Wesley, 1995.

American Petroleum Institution (API) Specification 16D Third Edition Draft: Control Systems for Drilling Well Control Equipment and Control Systems for Diverter Equipment. October 2014

NERC CIP Standards (North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP)) - Targeted at the energy sector

International Ship and Port Facility Security Code (ISPS) framework

15 Plans and Data *(1 June 2018)*

Industrial Control System – Functional Description Document (ICS-FDD)		
No.	*Title*	*Description*
1	Control Systems – FDDs	Current version of FDDs of control systems that are covered under the Cybersecurity Notation. General functional description. This document is to include the control system architecture (can be a separate document), software functions, Safety Instrumented System (SIS) & Essential Systems (ETS) designations to the individual functions and/or the control system, HMI/SCADA information. The functions are to have unique identifiers for traceability. *Ref. ABS ISQM Guide Section 9.* *Note: ETS & SIS maybe the same equipment. If so please indicate.*
2	Risk Analysis document	FMECA, FMEA, Safety Reviews, Failure case scenarios, etc., with risk ranking.
3	Control System Architecture	This document is to have line drawings of the control system, network topology, interface information, communication protocols information, new or unproven technology, and software version. *Ref. ABS ISQM Guide Section 9.*

Industrial Control System – Functional Description Document (ICS-FDD)		
No.	*Title*	*Description*
4	Equipment vendor list	This list has the manufacturer and the system provider's list for each control system under the CyberSafety assessment.
5	Management of Change (MOC) Document	Organization's MOC process, policies and procedures for asset ICS change management. This includes both software and hardware.

Cybersecurity Management System – Functional Description Document (CMS-FDD)		
No.	*Title*	*Description*
1	Cybersecurity Hardware list	List of equipment, version, manufacturer info, and other.
2	Risk Analysis document	FMECA, FMEA, Safety Reviews, Failure case analysis, etc., with risk ranking specific to Cybersecurity risk and failure scenarios.
3	Cybersecurity Control system Architecture	This document is to include details of the cybersecurity system implemented onboard the asset. It is to describe the functions with unique traceable identifiers, Safety Instrumented System (SIS) & Essential Systems (ETS) designations to the individual functions and/or the control system, HMI/SCADA monitoring information, performance metrics, Software information. *Note: The SIS/ETS designation is based on Cybersecurity Management System (CMS) failure that can affect or have impact on ICS that have SIS/ETS designation. ETS & SIS maybe the same equipment. If so please indicate.*
4	Network Architecture Document	This can be part of the Control system architecture. This document is to include network topology with unique traceable identifiers for each network, Interface and communication protocols for each network; Ports, Switches, Routers, Firewalls, Servers and all other network communication information that comprises the Cybersecurity Management System (CMS).
5	Organization Chart	Depicts the command path and authorization path within organization with roles and responsibilities. This can be specific only to the Cybersecurity team.
6	Cybersecurity Management of Change (MOC) Document	Organization's MOC process, policies and procedures for asset Cybersecurity system change management. This includes both software and hardware.

SECTION 2 The Cybersecurity Program

1 General

Cybersecurity is the application of security methods and controls to provide for, and to verify, deterministic behavior of cyber-enabled systems. A cybersecurity program is meant to safeguard assets, guide personnel and their actions, and allow freedom of action and of decision making within the boundaries of the system, free of interference from both internal and external influences. The cybersecurity process has a beginning but has no practical end short of decommissioning of the cyber-enabled asset.

Ship and offshore asset owners, operators and crew must understand their systems in order to use and protect systems, data, and asset functions. Poor cybersecurity can lead to loss of data or intellectual property; to loss of system integrity in both business-essential and business/mission/safety-critical systems; and to loss of system function in the critical control systems used to execute business processes. Cybersecurity can prevent losses when systems are designed, architected, engineered, built and operated with appropriate due care and due diligence.

Cybersecurity for systems must naturally provide security for people, data, systems and assets. Security for people must include periodic awareness training, systems training, and security policies and procedures. Security for assets includes the physical (ships, offshore assets, associated shoreside facilities and equipment) as well as the virtual (business data, process information, and intellectual property). But an organization's assets may also include its functions – those operations which keep the Company moving on its trajectory, which keep materiel flowing across production systems, or perhaps which keep raw materials moving through pipelines. Those functions that make the business viable are assets for the operation of the Company.

Systems that control production or operational systems, called operational technology (OT), are cyber-physical systems (CPS) that control processes and systems. These OTs or CPSs will have relevance to safety in their environments because they control direct physical effects in connected systems. They will often communicate with information technology (IT) general-purpose networks to provide sensor or operational data to management personnel. Because of the implications for CPS with safety consequences being connected to IT systems of differing trust levels, owners and operators require standards to which they can build and measure cybersecurity.

3 Process

The Company is responsible for setting the cybersecurity policies for the systems and ships/offshore assets it operates. As a minimum those policies must conform to international and domestic requirements, but they will also reflect the Company's objectives in maintaining safety and security onboard its vessels wherever they operate. The elements of a cybersecurity program include the following as minimum elements:

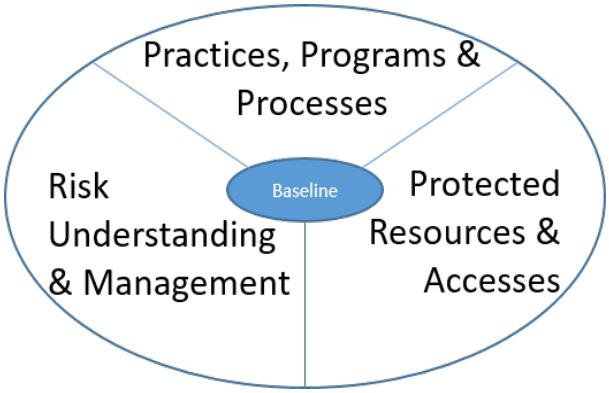
- Organizational capabilities suitable for defense from cyber threats;
- Risk assessment of cyber threats;
- Management system scope and depth suitable for defense from cyber threats; and
- System and equipment design and engineering to minimize cyber vulnerabilities.

ABS CyberSafety™ was developed to address these needs.

3.1 Organizational Capabilities

The ABS CyberSafety™ program is used to manage and measure levels of cybersecurity development, building organizational competence in defined capability areas. The capability areas encompass people, systems, processes and data, and form the core of organizational functions which implement the tasks and instantiate security controls. Organizational capabilities can be categorized into three related but distinct groups that describe the practices, programs and processes in a complete cybersecurity program. This is summarized in Section 2, Figure 1 below and more fully described in the ABS *Guidance Notes on Application of Cybersecurity Principles to Marine and Offshore Operations – ABS CyberSafety™ Volume 1*.

FIGURE 1
Categories of Capabilities within the ABS CyberSafety™ Model



Within the ABS CyberSafety™ model categories are the capabilities needed to achieve a measurable level of cybersecurity and CyberSafety. A capability is a functional approach to implementing a particular task set, combining people, systems, data and processes in order to execute a course of action in that capability area. Certain capabilities are required as a fundamental core to confirm the Company is prepared to move forward; these are the Baseline, noted above. Capabilities are built as the Company matures and brings more people, systems, data and processes into its operational environment.

3.3 Risk Assessment

Risk is the interplay among potential threats, Company assets, system vulnerabilities, impacts of incidents, and consequences of those incidents. The Guide requires and encourages understanding of risk conditions as part of the Basic Capability set (CS1), and as the Company expands and matures its cybersecurity program, this effort becomes risk management in the Developed Capability set (CS2).

A risk-based approach to cybersecurity in pursuit of CyberSafety entails the understanding of risk factors or risk conditions, with the business- or mission-based grasp of assets under risk. This allows prioritization of risk mitigation efforts, and it will guide the Company in building its security capabilities, implementing its security measures, and monitoring its security systems.

The Company must understand the value of its data and its intellectual property, and the value of its functional capabilities as enabled by cyber-physical systems. If control systems did not function correctly, and production machinery or processes ceased, the effect on the Company may be strong, no matter the source of the interference or interruption. Thus system function is considered an asset when working with control systems and operational technologies, especially in conjunction with cyber-enabled, safety-critical systems.

Assets may also include positive incentives as motivation for building capabilities, managing risks, and handling security. Data held in certain regulatory regimes, such as protected health information (PHI) or personally identifiable information (PII), or third-party data held by the Company, necessarily help the Company develop the prioritization of protections, tools and personnel assigned to protect those assets with Company systems. The Company's cybersecurity strategy, when based on risk assessment and risk understanding, will guide resource allocation in prioritization of tasks and capability development. When the most significant risk conditions or threat factors are used to develop and implement priority security controls, the Company is using a risk-based approach that can be measured and monitored.

3.5 Management Systems

The Company's Cybersecurity Management System is to address cyber security concerns and be subject to audit. Section 6 of this document defines the management system requirements for cybersecurity.

3.7 Systems and Equipment

3.7.1 Operational Technology

Operational Technology (OT) has been increasing in complexity and prominence for the last 30 years. Confusion resulting from blanket application of Information Technology (IT) management principles to an OT system is not only sub-optimal, but may very well be hazardous. Complex OT systems must be conceived, maintained, and tested quite differently than traditional IT networks and systems.

Increasingly OT systems are being connected to conventional (non-engineering) networks for monitoring, remote access or convenience. This exposes the OT systems to outside connectivity, potentially revealing vulnerabilities that could affect cyber-physical system operations.

The way forward relies on an understanding of the differences between OT-specific maritime cybersecurity and IT practices and appropriate handling. Policies and procedures must comprehend the differences in managing an OT network or system vs traditional IT methods.

3.7.2 Equipment Classification by Integrity Level and Potential Safety Impact

The judgment as to Integrity Level (IL) for safety-critical or safety-relevant systems will be considered in ABS CyberSafety™ assessments. Systems with direct safety impact within their systems, or secondary systems that could bring about potential failures in safety-critical systems, will be considered as requiring higher integrity levels than others that do not possess such features or functions. IL classification is in accordance with the ABS *Guide for Integrated Software Quality Management (ISQM)* and is represented as follows:

IL	*Potential Consequences*			*Examples, not inclusive*
	Safety	*Environmental*	*Functional*	
0	Negligible	Negligible	Minor impact on operation. Might affect supporting process system but not main process system	Entertainment System, Administrative computer systems, office network, Data Collection system (non-Authority required)
1	Might eventually lead to marginal safety incident	Might eventually lead to a marginal environmental incident	Might lead to maintenance shutdown of non-critical system. Main process continues to operate.	Non-essential control of systems, BPCS, Non-essential communication systems, Vessel Management System. New or unproven non-essential technologies minimum rating.
2	Within a short time could cause critical injury, lost time, accident or loss of a life.	Critical environmental impact	Shutdown of main system, excessive time for repair.	Drilling control system, BPCS, Safety Instrumented Systems (SIS) (minimum rating), PMS, essential systems, DP control system, main engine control system, safety systems, cargo control system, navigation system, new or unproven essential technologies minimum rating.
3	Immediate and Catastrophic lost time injuries, or multiple loss of life.	Catastrophic environmental impact	Significant repair time or loss of the marine or offshore asset.	Drilling Blowout Preventer control system, SIS or safety control systems, boiler firing control system, etc.

3.7.2 Security for All Components

Cybersecurity is generally focused on securing networks and devices on those networks. But other components must be included for defensibility and correct operations also. Transmission systems and lines must be safeguarded, whether by the Company or through its contracts with providers. Personnel must be trained for cyber-enabled system safety, resistance to criminal attack methods, and protection of organizational assets and critical systems or functions.

Resilience of critical systems is part of the cybersecurity implementation process. The result of resilience is that attacks or failures do not persist after incident response controls are executed and system restoration begun.

Defense in depth, the use of multiple means to view, protect and monitor networked assets, is an important part of resilience, as are architected solutions for designed-in resistance to unauthorized access or use; backup capabilities, such as redundant power or communications; user process definition as means to minimize errors or incorrect use; and system data restoration. Component security, with such features, helps confirm secure operational characteristics and integration with other systems in ways that do not introduce unexpected risks to the other systems. All these factors derive from the process and technology specifications in the Guide, combined with owner or operator insights or the assets protected.

3.7.3 Security and Remote Accessibility

Connections, communications and access to Internet Protocol (IP)-enabled sensors and systems that are considered components of the Internet of Things (IoT) or Industrial Internet of Things (IIoT) must be specifically addressed as part of the Operational Technology security measures onboard any ship, asset or facility. Remote accessibility to IoT/IIoT devices, especially, must be controlled carefully, as these devices are expected to be standalone, sealed, never-updated network participants, meaning that they can become conduits into primary networks if left exposed to unauthorized communications. These devices and similar systems are addressed in the OT specification in Section 5, with specific coverage under CS2's Capability 17.

Cloud storage and application providers also fall into the category for remote access. Authorized procedures for application and storage access must govern all communications with these offboard resources. Because of the nature of cloud communications, the primary protective requirements are human procedures and processes (such use of access control lists match against asset usage), with technical controls that specifically identify the user (two-factor or multi-factor authentication) when in contact with sensitive information systems or assets.

3.7.3 Management of Change for All Components

Notations in the **CS** series are dependent on owner/operator exercise of the capabilities as provided in the Guide, in addition to those capabilities and needs required by due diligence responsibilities, including management of change[6]. When a ship or asset is certified according to CS, ABS is to be notified when major changes are made to configurations or systems; when new interfaces between IT and OT are implemented, or existing interfaces are changed; or when new remote access methods are implemented for either IT or OT. ABS will communicate with the ship or asset management/owner, and with both IT and OT points of contact in these matters to confirm complete communications and understanding of changes and configurations.

[6] The ABS *Guide for Integrated Software Quality Management (ISQM)* provides additional guidance on Management of Change processes.

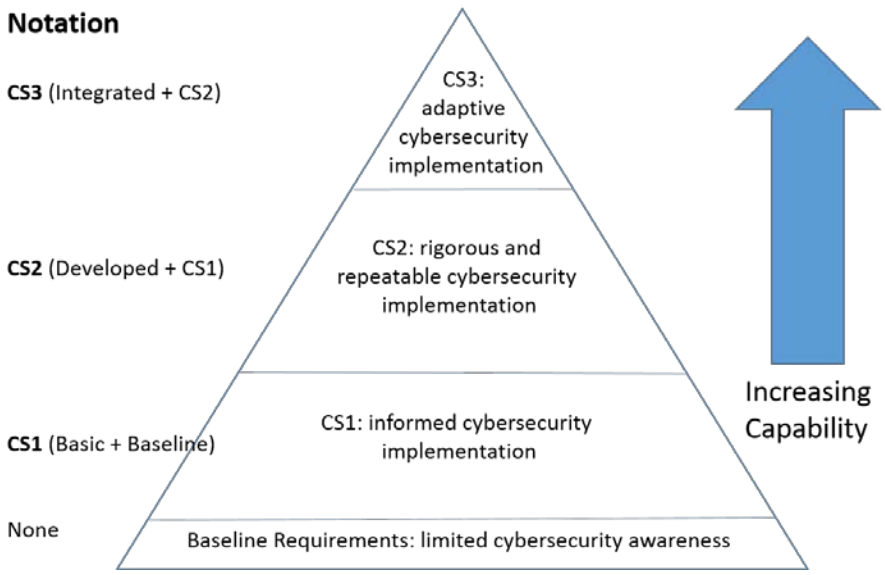
SECTION 3 Assessment of Cybersecurity Implementation for an Organization and its Assets

1 ABS CyberSafety™ Notation Implementation

This Guide differentiates organizations on two levels: first is the Company's implementation level or maturity, defined by the Notation assigned, and on the other level is the degree of implementation of the capabilities. Notations and capabilities combine as laid out below; capability implementation is the method the Company will use to move from one CS capability to another as it matures.

The ABS CyberSafety™ Notations provide context on how a Company views cybersecurity risk and the processes implemented to manage that risk, for either IT and/or OT. The Notations provide a method for gauging the relative thoroughness and rigor applied to cybersecurity risk management practices within the Company. It also provides the foundation by which ABS determines the robustness of the Company's cybersecurity protection and privacy protection programs. Section 3, Figure 1 below depicts the hierarchy of Notations:

FIGURE 1
Cybersecurity Notation Hierarchy



3.1 Baseline – Limited Cybersecurity Awareness Implementation (Lowest level of Readiness)

3.1.1 Risk Management Process and Process Documentation

The Company's IT and/or OT cybersecurity risk management practices are not formalized in the Company or aboard the asset, and risk is managed in an informal, reactive manner. Prioritization of cybersecurity and privacy protection may not be documented or based upon stated organizational risk objectives, the threat environment, business requirements, or the mission statement of the Company.

3.1.2 Formal Risk Management Program

The Company demonstrates limited awareness of cybersecurity risks at all levels of the Company, and a formal program for managing IT and/or OT cybersecurity risk is not evident. The Company's recognition and management of cybersecurity risks are guided by specific security incidents, and the response to those incidents is informed by external resources or internal resources that are not guided by job descriptions containing specialized cybersecurity knowledge. The Company does not have a permanent function implemented for managing cybersecurity incidents or communicating cybersecurity information within the Company.

3.1.3 External Participation

The Company has no formal process for coordinating, documenting or collaborating with external entities (e.g., other industry enterprises, international, federal, regional, and state authorities, class and certification bodies, etc.). This is important for IT, but it is a vital aspect of OT management and operations.

3.3 CS1 – Informed Cybersecurity Implementation (Basic)

3.3.1 Risk Management Process and Process Documentation *(15 June 2018)*

The Company's security and risk management practices are approved by internal management, and those practices are communicated in documented IT and/or OT policies and procedures. The Company's prioritization of cybersecurity activities is also evidenced by informed employees who are authorized and responsible for stating and managing documented organizational risk objectives, general and industry-specific threat environments, business/mission cybersecurity requirements, and cybersecurity regulatory imperatives.

3.3.2 Formal Risk Management Program

The Company documents and demonstrates an operational/organizational commitment to IT and/or OT cybersecurity within the Company. Risk-informed, management-approved ad hoc processes and procedures are defined and implemented, and staff has adequate resources to perform IT and/or OT cybersecurity duties. However, adherence to a documented cybersecurity reference model or framework is not evident. Cybersecurity information is informally shared within the Company.

3.3.3 External Participation

The Company can articulate its role in supporting or maintaining its' role in the maritime ecosystem, but has not formalized or documented its intention or capability for interacting with and sharing IT and/or OT cybersecurity information externally.

3.5 CS2 – Rigorous and Repeatable Cybersecurity Implementation (Developed)

3.5.1 Risk Management Process and Process Documentation

The Company's IT and/or OT risk management practices are formally approved and expressed as policies and procedures. OT cybersecurity practices are regularly updated based on the application of risk management processes, changes in business/mission requirements, and changes to the threat and technology landscape.

3.5.2 Formal Integrated Risk Management Program

The Company demonstrates and documents an organization-wide approach to managing IT and/or OT cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, internally verified, and routinely reviewed. Formal organizations and consistent, repeatable methods are in place to respond effectively to changes in risk. Cybersecurity risk management activities are documented for review by internal and external assessment organizations. Cybersecurity activities are resourced, and responsible personnel possess the knowledge and skills to perform their appointed IT and/or OT protection roles and responsibilities.

3.5.3 External Participation

The Company understands its dependency upon informed agencies and partners, and receives information from these agencies and partners that enables collaboration and informed risk-based management decisions within the Company to respond to OT cybersecurity events.

3.7 CS3 – Adaptive Cybersecurity Implementation (Highest level of Readiness) (Integrated)

3.7.1 Risk Management Process and Process Documentation

The Company adapts its IT and/or OT cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the Company actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.

3.7.2 Formal Integrated Risk Management Program

There is a Company-wide approach to managing cybersecurity risk that uses formal documented risk-informed policies, processes, and procedures to address potential cybersecurity events. Formal OT cybersecurity risk management organizational functions and general organizational awareness are demonstrably part of the organizational culture as derived from an awareness of embedded activities, information shared by other sources, and continuous awareness of activities on the Company's internal and linked systems and networks.

3.7.3 External Participation

The Company maintains internal expertise on IT and/or OT cybersecurity concerns, manages risks based on cybersecurity data and acquired intelligence, and actively shares information with partners to confirm that accurate, current information is being distributed and consumed to improve cybersecurity before an IT and/or OT cybersecurity event occurs.

3.9 Applicability of Capabilities to Asset Protection

Organizational capabilities give sustainability to the security protections, methods, systems and controls put into place to protect the Company's assets. Protected systems are mapped by the Company into the capabilities as they are operationally provided in the chosen levels (CS1-CS3) to run the Company, business, mission, etc.

Protected operational technology and information technology assets are directly connected to the requirements set forth as part of each capability specification. Potential failure modes and potential threats are to be considered within the context of each Company's environment, and as well within the context of the systems' installation environments[7].

Organizational capabilities provide supportable, maintainable means to provide security and soundness of operations over time. The emphasis in building the capability levels for Notation is to provide the Company a sustainable program for security in multiple aspects (i.e., using many capabilities for holistic security) that allows deliberate decisions about resource allocation, relative risk and protective controls. The capabilities within a Notation may not be the only capabilities required to protect organizational assets. Further capabilities may be prudently chosen to complement a Notation in order to tailor Company resources and effort to its relative risk, given its assets[8].

5 Applicability of Notations and Certifications *(15 June 2018)*

i) ABS Class Notation for a ship or offshore asset, as applicable, will indicate **CS1**, **CS2**, or **CS3** based on protections and Company capabilities to support those protections for minimum sufficient security of the asset. The Notation will indicate **CS1+**, **CS2+**, or **CS3+** if the Company has an ABS Cyber Certificate (i.e., the Company has undergone ABS CyberSafety™ assessment for its related facility/facilities as well). The Notation **CS-Ready** indicates compliance with Section 8 of this Guide.

[7] Operator errors can contribute to system failures, and the designed installation environment may alleviate some potential errors by removal of failure modes.

[8] For example, a Company may certify a ship at CS1 (capabilities 1-9), but Company leadership may decide that implementing capabilities 16 (data security) and 17 (operational technology protection) is prudent for their relative risk position. The intent of the severable capabilities is to allow choices for flexibility and consistency in accord with organizational environment and situation, rather than to satisfy a particular stated list of tasks.

ii) The CyberSafety Management System Certificate (CMSC) will list those systems, equipment, networks and interfaces assessed. The CMSC will denote the current status of the ship or system(s), indicate any areas for continued attention, and the periodicity requirement for next inspection or assessment.

iii) The Certificate of CyberSafety Compliance (CCC), provided to a Company for assessed facilities, will provide similar scope and content as CMSC, but tailored to the facility under assessment.

Additional scope of a Notation beyond specified Notation requirements, in the event of capabilities required by circumstance above a particular level of Notation, will be recorded in comments and verification plan for the Notation. Additional assets, such as Well Control, will be handled on a case-by-case basis.

7 Safety of Personnel and Equipment

Safety of personnel and equipment are to be considered by the Company and the Surveyor reflected in:

i) The cybersecurity assessment and test plans, equipment setup, and other activities at the testing location (at factory or onboard) for safety of personnel and protection of equipment and the environment during execution of the Cybersecurity Assessment.

ii) The re-activation of the system(s), from testing state to normal, controlling equipment for safety of personnel, equipment, and the environment.

Tests deemed to violate 3/7i) or 3/7ii) are either to have risk mitigated or the test is not to be performed.

9 Onboard Testing

While the control system is installed onboard and testing is to be performed, the Owner, SBI, and Verification and Validation (V&V) personnel are to agree on the functions or functionality to be tested and the safe method to perform the testing.

Tests or scenarios identified as having risk to safety, environmental, or equipment impacts damage are not to be tested onboard.

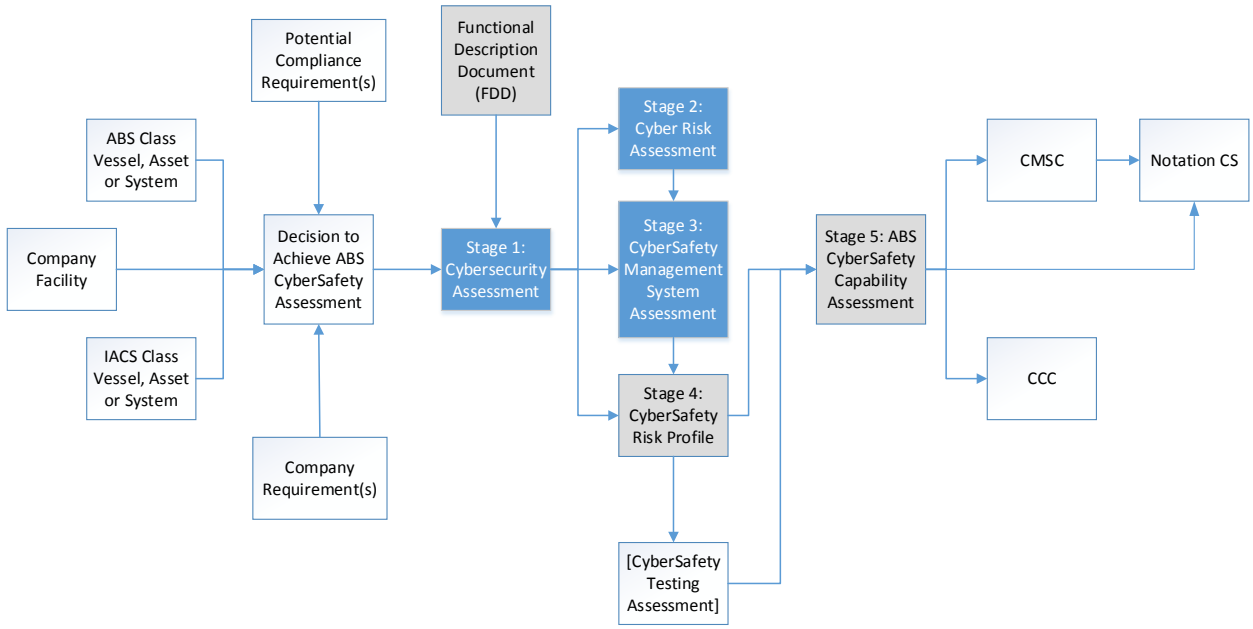
The Surveyor is to observe onboard testing and testing results as identified by test plans and scenarios. The Surveyor will not participate in any other role during testing.

11 Capability Assessment Process *(1 June 2018)*

The assessment process requires development of a stage-wise risk profile for the ship, asset or facility, following the engagement path shown in Section 3, Figure 2 below.

An initial ship or asset assessment will be a multi-part event that may be conducted in one contiguous time period, if ship or asset personnel and documentation are available, or it may be broken into parts to better match Company needs. Each stage will encompass specific objectives and will deliver products particular to those objectives. The expected outcome of the entire process is a capability assessment that shows any remaining gaps or decisions required to satisfy the Company's cyber-enabled systems safety and security requirements, along with the appropriate certificate or Notation when the process is complete to ABS and Company satisfaction.

FIGURE 2
Capability Assessment Process *(1 June 2018)*



11.1 Company Decision Stages

The left side (unshaded) of Section 3, Figure 2 shows several portions of the decision process that leads to the ABS CyberSafety™ certification. The Company decides what assets, vessels or facilities will be addressed in certification. Potential compliance requirements that may modify assessment needs, along with Company requirements for cybersecurity[9], will contribute to this decision to pursue the certification process.

11.3 Stage 1: Cybersecurity Assessment

The initial Cybersecurity Assessment includes asset enumeration, policies and procedures examination, architectural documentation examination, and asset comparison with the Functional Description Document (FDD).

11.3.1 Functional Description Document

The FDD is the combined documentation associated with architecture, operations, security and testing of the mission-critical or business-critical systems aboard a ship, on an offshore asset, or in a facility. The expected content of an FDD is provided in Subsection 3/13 below.

11.3.2 CyberSafety Management Plan (CSMP)

The CSMP is a mid-way stage to establish a CyberSafety Management System (CSMS) if the Company does not have a method set in place to manage its critical systems' cybersecurity and safety postures. The CSMP is a work breakdown structure (WBS)-oriented program to develop and implement a capabilities-based CyberSafety program.

11.5 Stage 2: CyberSafety Risk Assessment (CRA)

Stage 2 includes asset risk condition assessment, with a functional protective measures comparison against Company requirements. Threat matching with the protective measures will reveal any gaps the Company may have. The stage provides an Initial Risk Profile at conclusion.

11.7 Stage 3: CyberSafety Management System Assessment (CMSA)

Stage 3 assesses the Company's cybersecurity management across the organization and its assets, including automation methods, asset management and comparisons with the FDD, and cyber-related systems management and reporting. This stage provides templates and tools, as required.

[9] Internal requirements may flow from security or technology strategy, policies in place, or other expectations that the Company decides to include in the process.

11.9 Stage 4: CyberSafety Risk Profile Development (CRPD)

Stage 4 compiles all management system, asset assessments and risk assessment outputs to develop the Company Risk Profile. This uses the risk progression developed through previous stages to provide a measurable achievement profile for continued progress toward capability set certification.

11.11 Stage 5: CyberSafety Capability Assessment (CCA)

The CCA includes capability assessment, FDD assessment, interfacing systems assessment, networked systems audit, data integrity assessment and final certification for either CCC or CMSC and Notation.

13 Functional Description Document (FDD) and Document Submission Requirements

To support proper review in ABS CyberSafety™ assessments, the following documents are to be available to ABS for review. These documents comprise the Functional Description Document (FDD) in a constructive form, and they provide the visibility and understanding required for system assessment.

Documents and named artifacts include many such as the following:

- Integrity level reviews
- Safety Instrumented Systems (SIS) functions and status
- Failure Mode, Effects and Criticality Analysis (FMECA) records and updates (upon major configuration changes)
- Test reports and documentation, with retests
- Data logs from control systems
- Operations and Maintenance (O&M) Plan
- Control Equipment Registry
- Software Registry
- Software Management of Change (SMoC) Plan, Policy and Process
- Software Change Management Plan (CM)
- Software Configuration Management Plan, Policy and Process

Other documents commonly contain valuable data supporting documented processes and operational test results. Documents containing the following data are also to be available:

- Conditional states
- Integrity levels of components/systems
- Production system interfaces
- Human-Machine Interface (HMI) instructions
- Software versions, firmware, hardware by spec
- Constraints on system operations, with reasons
- All other interfaces (non-HMI, Supervisory Control and Data Acquisition (SCADA), data collection, with protocols and constraints)
- System conflicts and unresolved software issues
- Hardware and software obsolescence plans
- Reliability, Availability, Maintainability and Supportability (RAM-S) reviews
- Safety reviews

SECTION 4 Requirements for Certification

1 Categorization of Security Program

Security programs fall into the following general categories:

- *New Construction Asset.* New development of a security program with a new asset (marine, offshore or interfacing facility) in accordance with the owning Company's security and other guidelines and requirements.
- *New System.* Development of security for a new system, application or appliance, to be incorporated or integrated into an asset (marine or offshore) security program with either an existing or a new security program in effect.
- *Legacy Asset.* Existing system of system (ship, offshore platform, or other maritime asset with multiple existing standalone and networked systems) upon which a security program must be overlaid in accordance with organizational security and governance needs.
- *Legacy System.* Existing system for functional contribution to a legacy asset, new construction asset, or an interfacing facility, which may be networked or standalone.

3 Requirements and Capabilities Required for ABS CyberSafety™ Notation/Certification *(1 June 2018)*

A Company will build and provide capabilities to enable security in the Company. These capabilities provide continuous support for the security facets appropriate to the Company's security strategy. Assessment by ABS measures the scope and depth of those capabilities. An organization under assessment for CS1 (Basic), CS2 (Developed), or CS3 (Integrated) level certification is to demonstrate that:

i) The Baseline requirements are met as a foundation for building Company capabilities for supportable, understandable and measurable cybersecurity;

ii) The capabilities included in the level for certification are provided, supported and maintained by the Company;

iii) The Company has tailored any further capabilities required – even if they are not part of the certification process in consideration – to confirm completeness of security;

iv) The capability and its related specifications for Operational Technology have been considered and applied where appropriate for the process control and OT aspects of its architecture that have contact with, or impact upon, human safety-related conditions; and

v) The security specifications, conditions and controls applicable under specific capabilities are implemented and monitorable/monitored as required to maintain security appropriate to the risk conditions understood in the Company.

The capabilities in all Sets bring rules with them, and it is important to understand that building and sustaining capabilities will require governance guidelines for consistent maintenance.

- Prioritization of security efforts across an Company can be accomplished with the levels provided in this Guide. Security for any particular organization must be tailored to its individual conditions, assets to be protected, risk conditions, and security threats. An implementing Company may choose to certify at Basic level, while needing to provide security from capabilities in the Developed level as well.

- Capabilities determine effective application of security controls and techniques. Capabilities determine effectiveness and sustainability of security measures in place in any Company's environment.
- A Company with a given level of certification, but with assets or operational needs in excess of that level, may require policy statements to guide their employees and system users that exceed minimum requirements for their certification level.

Assessment and grading a Company entails a two-fold evaluation, including security measures in place, and the Company's ability to support, sustain and maintain those measures or capabilities. Best-in-class organizations understand their assets and installed base, monitor those assets and the personnel or machines allowed to access them, and provide ready feedback for continuous improvement. Companies with these characteristics will have better systemic resilience and overall recovery capability due to increased self-knowledge and reduced uncertainty concerning assets, threats, and weaknesses present in their systems.

A Company under assessment may have differing levels of Notation among vessels, and it may have a different level of certification granted when the Company assesses its facility or facilities. Each vessel will earn Notation on its own merits, and the Notation will reflect in the vessel's ABS *Record*. Control systems assessed within the scope of the **CS** notation will be listed in the ABS *Record*. Vessels, not requesting CyberSafety™ notations, may receive the CyberSafety Management System Certificate (CMSC) as noted previously, which will show systems and cyber-enabled equipment assessed within the scope.

The Company's Certificate of Cyber Compliance (CCC) will provide similar information as the CMSC, but for the assessed facility. If both Company and vessel(s) are assessed, vessel Notations will reflect on the highest successful Notation level achieved, as will the facility; there need not be level consistency between or among them. The vessel Notation would reflect as **CS(1/2/3)+** to denote that the Company was also assessed to the Guide specifications.

5 Specific Requirements and Capabilities for Operational Technology

A Company with mission-critical OT installed and functioning, whether aboard ship, platform or in facility, is obliged to protect the OT systems as part of their due care and due diligence associated with corporate governance, regulatory compliance, personnel safety, and asset protection needs. Because OT is frequently considered to be apart from, or separate from, information technology (IT), but often connected to IT for monitoring, remote access and control purposes, it is imperative that the process control systems, or cyber-physical systems, be protected both physically and logically.

The Company is to use appropriate regulatory and reference materials to determine their security posture. The OT specification portion of the Section 5 Capability Matrix is to address the major components of OT security and is intended to guide implementation of OT installations and operations. In developing the criteria, industry standard publications (e.g., IEC 62443, NIST Special Publication 800-82r2) are to be referenced for technical detail as required, as appropriate for the arrangement utilized. An assessment version of the OT specification, mapped to applicable industry standards (i.e., IEC 62443 and NIST Cybersecurity Framework), is to be available separately as an additional resource for OT security, to be provided as a Guidance Note for self-assessment or survey.

7 Use of the Capability Matrix

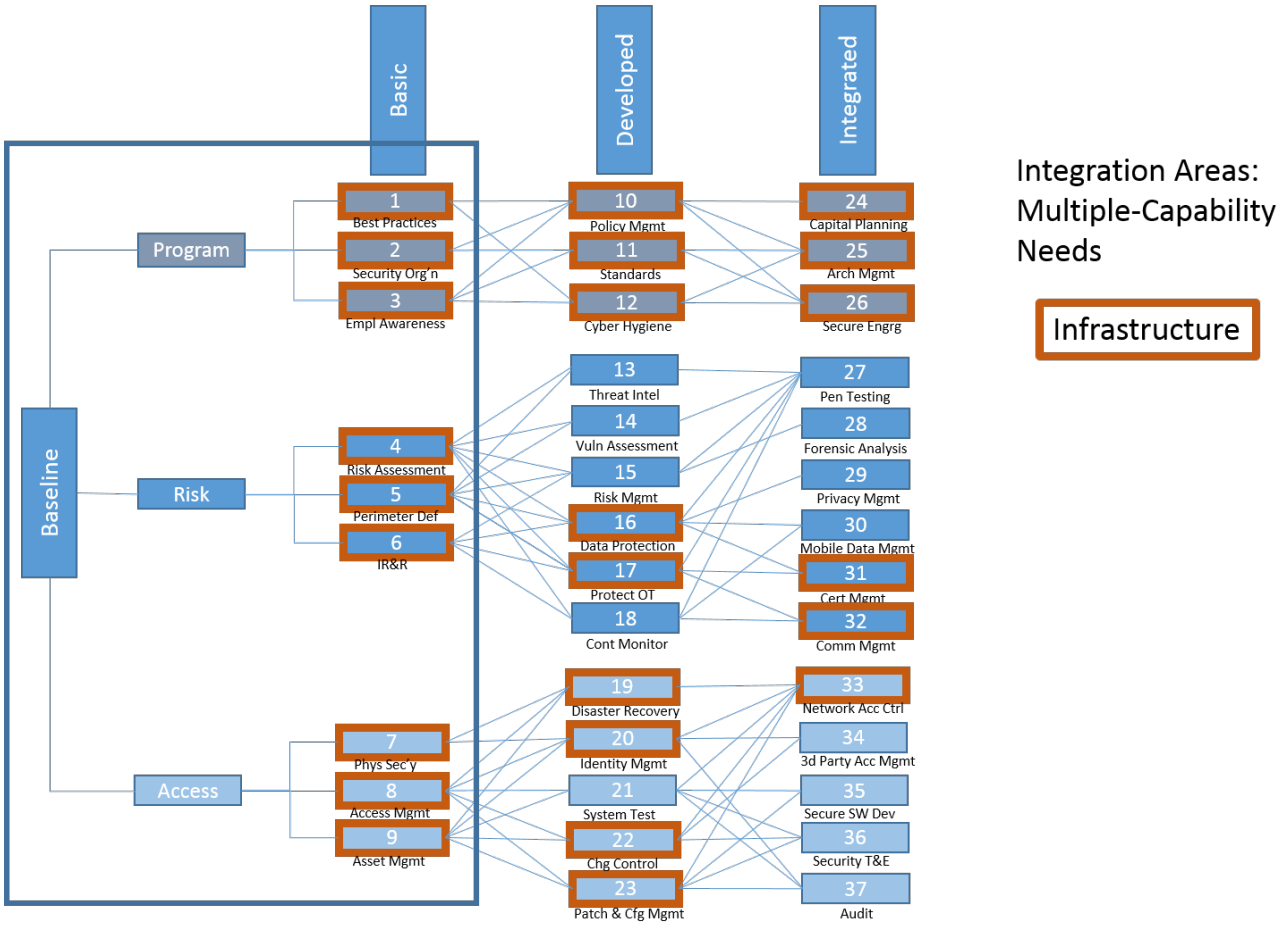
The Capability Matrix, in Section 5 herein, establishes marine- and offshore-specific best practices, defining and providing the organizational process specification for each capability together with the associated IT and OT specifications.

- Best practices frame the context for the individual capabilities. These notes encapsulate lessons learned and practices that are current in the capability area under examination.
- Process specifications detail how the Company may structure itself to accomplish and provide the capability in an operational setting. This specification set provides requirements for determining and shaping what the organization requires as human or system processes to implement both best practices and the technology specifications.

- The IT specification lists those requirements associated with implementation of IT within that capability. The technology specifications relate to previous capabilities, where applicable, to provide completeness through the scope from less to more complex capabilities.
- The OT specification provides those requirements associated with development, engineering and operation of OT within each capability.

To illustrate potential relationships, Section 4, Figure 1 below shows how the capability sets can connect and relate in a particular, generic implementation.

FIGURE 1
Capability Sets in Relationship to One Another



The Baseline and Basic capability sets are minimum requirements for an organization to satisfy Cybersecurity.

In this illustration, the three major subdivisions divide into the capabilities within those specific areas. The color scheme in shades of blue is meant to show commonality in each area for differentiation only.

In the Program category, for example, the Basic capability set includes Best Practices, Security Organization and Employee Awareness. These expand into the Developed level to require Policy Management, Standards, and Cyber Hygiene, then into Integrated level capabilities to include Capital Planning, Architecture Management and Security Engineering.

Each category expands from less complex capabilities into more complex capabilities, building into the Integrated set that each require inputs from several subordinate capability areas. As an example, Integrated capability 27 (Penetration Testing), when executed correctly, will derive from and integrate Perimeter Defenses (5), Threat Intelligence (13), Vulnerability Assessment (14), and System Test (21) to provide the best results. Similarly, Integrated capability 29 (Privacy Management) will combine elements of Perimeter Defenses (5), Risk Management (15), Data Protection (16) and Identity Management (20) for a complete solution.

Capabilities requirements will develop differently based on organizational needs. Some organizational development may require capabilities outside particular sets in order to address risk factors present in a specific context. In that case, the basic set of capabilities is required, along with those capabilities needed to address the risk(s) for that Company.

The Basic Capability set (including the Baseline) is the minimum requirement for a Company to satisfy Cyber due care and due diligence for the technology systems. But additional requirements may apply to an organization in its specific and unique environment. Section 4, Figure 1 above is an illustration of what capabilities may be required to satisfy security in a view toward secure infrastructure operations and management. Several Developed capabilities, and additional integrated capabilities, are shown highlighted as potential needs for the Company to operate with a degree of measurable completeness.

Specific additional "views" in a Company may require other combinations of capabilities for needs coverage. A security operations view requires additional, and different capabilities than will the secure infrastructure operations view shown.

The size of the Company, personnel complement, and numbers of fielded technology systems will drive the level of CyberSafety assessment, accomplishment and certification required to understand the Company's security position and posture. Smaller Companies with relatively small numbers of IT and/or OT systems may be satisfied to implement and certify to the Basic level. Larger organizations with more complex systems, operations or relationships may require an implementation at the Developed level, or CS2. Large, complex Companies will probably require implementation at the Integrated level, CS3, to better accommodate their multiple needs across many subordinate organizations, units or assets.

SECTION 5 ABS CyberSafety™ Capability Matrix

1 Capability Matrix

The following tables provide the specifications necessary to satisfy Baseline, CS1/Basic, CS2/Developed and CS3/Integrated capability levels.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
Baseline Requirements			
1- Practices, Programs, and Processes			
(1) Exercise Best Practices			
(2) Build the Security Organization	PB2-1 The Company has personnel assigned to confirm assets and systems are received and installed in accordance with positive control and inventory or tracking procedures. PB2-2 The Company provides spaces for security personnel and operations, and security containers, safes or safe storage methods for secure storage or security data, devices or materials.	ITB2-1 Personnel are positively identified for information technology and data system duties and security, with appointment letters as required.	OTB2-1 Personnel are positively identified for operational and process control technology duties and security, with appointment letters as required.
(3) Provision for Employee Awareness and Training	PB3-1 Use broadcast emails for threat awareness and reminders of good practice. PB3-2 Employee basic training process is annual or as required, tracked and managed, and it includes • Initial (and refresher) cybersecurity training and awareness • Technology acceptable use policy, with signature • Social media training • Social engineering (Phishing, Vishing and Smishing) familiarization for threat awareness • Web use hygiene habits	ITB3-1 All users will receive standard notification banner for acceptable use and business purposes when logging into their enterprise-owned machines.	OTB3-1 All users will receive standard notification banner for acceptable use and business purposes when logging into operational, process-control systems or into interface machines that connect to operational technology systems.
2- Risk Understanding and Management			
(4) Perform Risk Assessment	PB4-1 The Company conducts periodic, or at least annual, risk assessment of current assets and risk position in their context or environment. PB4-2 The Company understands those systems, functions or data which is completely critical to safe operation of systems or assets.	ITB4-1 Perform annual (or more frequent) inventory of network-enabled and network-connected IT assets and systems.	OTB4-1 Perform annual (or more frequent) inventory of network-enabled and network-connected OT and cyber-enabled functional assets.
(5) Provide Perimeter Defense	PB5-1 Any system, workstation or device will have any inherent protective systems activated by default.	ITB5-1 Workstation or device protective systems or built-in firewalls, either hardware-based or operating system utilities, are activated by default prior to placing any system into the Company's networked environment.	OTB5-1 No system, module, component, appliance, device or application will be allowed to communicate, whether through the network or out-of-band, without explicit permission from the Company.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	PB5-2 No system, module, component, appliance, device or application is allowed to monitor its operator, whether by camera, microphone or keyboard capture, without conscious permission of the Company or the operator. PB5-3 Every server, system, appliance, module, component, device or application will be installed with password access, and passwords shall be stored in a safeguarded location in the Company.	ITB5-2 Communication utilities in workstations or end-user systems are positively managed to confirm only authorized users control access to cameras, microphones and speakers. ITB5-3 Network infrastructure devices, especially commodity procurements, are not installed and activated in networked environments until their default protective mechanisms and methods are activated, and default accesses and passwords are changed.	OTB5-2 No operational technology or process control system is directly connected to the Internet. OTB5-3 New devices or sensors (i.e., Industrial Internet of Things (IIoT)) will be tested for performance, potential system impact and secure access methods prior to installation in operational systems.
(6) Prepare for Incident Response and Recovery	PB6-1 The Company has a process defined by which positive control of systems can be regained and personnel and asset safety maintained. PB6-2 All safety-critical systems have manual backup capabilities installed, and personnel are periodically trained in use of manual backup systems and methods.	ITB6-1 All enterprise or organizational systems have data backup and recovery capabilities installed and enabled. ITB6-2 All enterprise or organizational systems have system software master copies kept in safe storage for emergency system recovery / reload purposes.	OTB6-1 All enterprise or organizational OT and control systems have data backup and recovery capabilities installed and enabled, as appropriate. OTB6-2 All enterprise or organizational process control systems have system software master copies kept in safe storage for emergency system recovery / reload purposes.
3- Protected Resources and Accesses			
(7) Provide Physical Security	PB7-1 The enterprise physically controls all network resources within its boundaries and area of control, including portable systems or devices and network connections. PB7-2 The Company limits options for system access, device or data theft, or human information leakage by controlling visitor access in areas where unattended presence is possible, or where inadvertent eavesdropping could reveal Company operations or details. PB7-3 Video feeds from installed surveillance systems, especially Internet Protocol (IP) cameras, are not available to unauthorized or non-authenticated access. PB7-4 Manual backup methods for control of safety-critical systems are safeguarded in the same ways as are primary and automated controls in those systems. PB7-5 USB data storage or transfer devices are prohibited from physical access or use by policy, except in specified, allowed circumstances.	ITB7-1 Access control lists (ACLs) for physical possession or contact with system assets (devices, systems, workstations, servers, network connections, etc.) are established and kept up to date. ITB7-2 Physical access to spaces containing IT assets is controlled by physical barriers and devices (doors, locks) and governed in accordance with ACLs. ITB7-3 Common interface ports used for power (i.e., charging portable devices) are provided as power outlets in Company spaces in order to remove possible avenues for unauthorized or high-risk access to systems, appliances, workstations or devices. ITB7-4 Portable devices (laptops) are protected against data theft or illicit access via stolen machines by use of whole-disk encryption. ITB7-5 Infrastructure devices shall include tamper-evident seals on critical components within safety-critical or safety-relevant systems.	OTB7-1 Access control lists (ACLs) for physical contact with system assets (devices, systems, workstations, programmable logic controllers, network protocol translators, network connections, etc.) are established and kept up to date. OTB7-2 Physical access to spaces containing OT assets is controlled by physical barriers and devices (doors, locks) and governed in accordance with ACLs. OTB7-3 The Company prevents, both by policy and by physical or logical means, the ability for inappropriate and unauthorized portable device connections to OT/ICS.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
(8) Execute Access Management	PB8-1 New infrastructure systems shall be prepared for installation for network resource access in accordance with organizational baseline policies and procedures. PB8-2 Local (serial) connection methods are to be used, where possible, for configuration and administration tasks for infrastructure devices. PB8-3 New endpoints or user access devices shall be prepared for installation in accordance with organizational asset baseline policies and procedures. PB8-4 Personnel access to networked resources is governed by the principle of least privilege; access granted is the minimum necessary for personnel to perform their stated and defined duties.	ITB8-1 Infrastructure systems, devices, serves, applications and assets are initially configured to remove all default settings prior to installation in the networked environment, including: • Vendor default passwords are to be changed; • Administrator account passwords or access accounts are positively set upon system receipt and installation; • Administrator passwords are non-trivial and tracked by secure means in Company; • Remote access is configured only if specifically required, not be default; and • All system accesses will be tracked by logging, by unambiguous login identity or credential, to main or auxiliary repositories that contain enterprise data of consequence. ITB8-2 User endpoint systems, devices, applications and assets are initially configured to remove all default settings prior to installation in the networked environment, including: • Vendor default passwords will be changed; • Administrative privileges are not granted as to ordinary user accounts by default; • Endpoints have lateral network access or visibility only within the immediate area of their functional requirements, without default access to other systems or assets on the network; • Single sign-on (SSO) is configured for applications as required; and • Preconfigured software that uses OEM or manufacturer call-out methods will be disabled in the standard user profile to prevent unauthorized communications.	OTB8-1 All operational technology or process control system components, systems, modules, applications or appliances will have default passwords changed prior to their being activated in the Company's process control network. OTB8-2 All operational technology or process control system components, systems, modules, applications or appliances will have any remote access methods established with two-factor authentication, nontrivial passwords, and access control lists (ACLs). OTB8-3 All operational technology or process control system components, systems, modules, applications or appliances will have protocols and services (including Secure Shell (SSH)) secured against unauthorized access. OTB8-4 All operational technology or process control system components, systems, modules, applications or appliances will implement verbose logging to allow tracking of user access; resources, source IP, time/date, and files or systems accessed. OTB8-5 No operational technology or process control system components, systems, modules, applications or appliances will be configured to allow cellular data access, either one-way reporting or two-way query-response, without written permission of the asset owner. OTB8-6 No access to OT systems via USB port is allowed without prior testing of the device and/or data to be transferred by that port.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		ITB8-3 Network access regulation includes the following: • Organizational network connections (Ethernet) are disabled at switches unless specifically intended for use; • Wireless network (WLAN) requires login credentials for use; and • Access to the organizational WLAN connected to enterprise network resources is limited to Company computing assets only. ITB8-4 Networked system access by users or systems shall be logged and maintained for an organizationally-determined period, showing user access by resources accessed, source IP, time/date, files accessed.	
(9) Maintain Asset Management	PB9-1 The Company maintains positive management of assets through inventory and asset tracking methods per installation, facility, platform or employee. PB9-2 The Company configures all non-safety-related systems to lock screens after an organization-determined time-out period to prevent casual, unauthorized access to systems, software and data. PB9-3 The Company treats data and digital property with the same considerations and conditions as are applied to physical assets, using access control lists (ACLs) and need-to-know criteria for access. PB9-4 The Company tracks licensed software and authorized software on networked or enterprise-owned machines.	ITB9-1 All computational assets receive uniform treatment to provide them the following characteristics: • Baseline software load (approved load, or 'gold disk') of approved software, with all other software removed • Administrator accounts are hidden or removed • Machine identification is assigned, and Media Access Control (MAC) address and Network Interface Card (NIC) hardware identifiers are recorded as part of asset controls. • Basic antivirus and/or anti-malware protection is installed as part of basic software load. ITB9-2 Networked devices, such as multi-function printers, are configured upon installation to remove services not used, insecure services, and remote access prior to full activation. ITB9-3 The Company places critical data (identified in Risk Assessment) in secure storage with designated, accountable, tracked access.	OTB9-1 Operations-critical or safety-critical systems are specifically configured to lock screens, interfaces or operator accesses only on conscious action by operators or administrator personnel. OTB9-2 The Company maintains active and accurate OT and process control systems inventories, including software versions and relevant software utilities or applications necessary to operation of the OT or process control systems. OTB9-3 The Company maintains current OT and process control systems software in controlled access libraries to support onboard OT, and provide reversion to known-good software loads when necessary. OTB9-4 OT and process control system data streams and data stores or repositories are governed by the same access control processes as other critical resources, requiring ACLs and credential-based access for critical data.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
CS1: Basic Capability Specification			
1- Practices, Programs, and Processes			
(1) Exercise Best Practices ***Best Practices Include*** *The Company maintains relationships with information sharing communities and threat or vulnerability broadcasts from both governmental and industry sources.* *The Company shares threat information with peers in its community, including technical information such as indicators of compromise (IoC), to promote greater awareness and community resistance to attacks.* *The Company uses regional and national resources (e.g., US-CERT, ICS-CERT and ENISA) to gain access to recent vulnerability and threat information relevant to its assets.* *The Company builds a series of cultural practices that include cybersecurity requirements, thereby promoting due care and due diligence continue on a routine basis.* *The Company actively engages, trains and informs its Board of Directors, or similar leadership structures and personnel, on cybersecurity practices, potential impacts of cybersecurity risks, and ongoing issues due to cybersecurity in the Company's environment and context.*	***Process Specification Requirement*** P1-1 The Company participates in information sharing communities, both governmental and industrial, for cybersecurity vulnerabilities, threats, threat methods, Indicators of Compromise (IoC), attack resistance methods, and risk sources. P1-2 The Company promulgates best practices from community involvement or broadcasts to its personnel to confirm those lessons learned can become part of the Company's practices, processes and procedures. P1-3 The Company confirms best practices and lessons learned are provided to policy and standards administration to incorporate Company-specific guidance into the directives, instructions and process guides that govern organizational operations. P1-4 Best practices and lessons learned are fed forward into risk assessment and risk management processes. P1-5 The Company monitors relevant industry risk management regulations and public policy.	***Information Technology Specification Requirements*** IT1-1 IT threat information sources are identified, received, reviewed, recorded and correlated against installed and required assets in a regular routine in the organization. IT1-2 IT threat information sources include governmental sources (e.g., US DHS, US-CERT), community and collaborative sources (e.g., US InfraGard), industry groups, and vendor or other expert groups. IT1-3 IT lessons learned and threat information source information is regularly provided to organizational personnel to confirm understanding and integration of lessons to improve organizational practices.	***Operational Technology Specification Requirements*** OT1-1 OT threat information sources are identified, received, reviewed, recorded and correlated against installed and required assets in a regular routine in the Company. OT1-2 OT threat information sources include governmental sources (e.g., US DHS, ICS-CERT), community and collaborative sources (e.g., US InfraGard), industry groups, and vendor or other expert groups. OT1-3 OT lessons learned and threat information source information is regularly provided to organizational OT, process control and field systems personnel to confirm understanding and integration of lessons to improve organizational practices. OT1-4 The Company tracks, monitors and communicates production system risks and incident management plans to other organizations that could potentially be affected by security incidents or security system changes.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
(2) Build the Security Organization ***Best Practices Include*** *The Company matches tasks to required skills, building employee skill for long-term development of experience and institutional knowledge.* *The Company performs periodic capability assessments to confirm that organizational leadership understands current security status, personnel and organizational capabilities, and gaps in processes, staffing or systems.* *The Company possesses a security strategy that informs and influences its technology strategy, and both strategies in turn support business requirements and staffing to sustain security conditions and postures.*	***Process Specification Requirement*** P2-1 The Company provides personnel and specific functions, responsibilities, authorities and accountability measures to implement and support information security within and across the entirety of the Company, with specific personnel designated for local or unit responsibilities as required to maintain security postures. P2-2 The Company's senior management team includes a Chief Information Security Officer (CISO or equivalent) who is empowered to implement the information and data security program within the enterprise, and accountable for that program's outcomes. P2-3 Organizational security personnel job positions are staffed in accordance with industry standards for numbers, assets, units, and relative threats and/or risks, taking account of automation methods and information gathering and sharing requirements. P2-4 The Company establishes and maintains a Security Roadmap, establishing a current state of security and technology, and an expected progression of security technologies and processes to match or pace both known and potential threats. P2-5 The Company assigns a specific person to be responsible for cybersecurity for occasions when the ship or asset is out of service, in long-term maintenance, or out of normal operations.	***Information Technology Specification Requirements*** IT2-1 Personnel are positively identified for information technology and data system duties and security, with appointment letters as required. IT2-2 Security personnel structures are matched against responsibilities and system monitoring needs to justify personnel or staffing requirements. IT2-3 Security staffing duties are assigned by organizational priority and by identified risk areas or conditions. IT2-4 Security staff training paths are identified in the Security Roadmap, supporting and maintaining a relevant, vibrant, learning Company to best support the Company against known or potential threats.	***Operational Technology Specification Requirements*** OT2-1 The Company establishes and maintains an ICS Security Office to provide operational availability and continuity, to direct implementation of ICS security, to direct ICS security activities, and to administer the Cybersecurity Management System (CMS) aboard each offshore or marine asset, or in each facility housing OT systems. OT2-1 Personnel are positively identified for operational and process control technology duties and security, with appointment letters as required. OT2-2 Security personnel structures are matched against responsibilities and system monitoring needs to justify personnel or staffing requirements. OT2-3 Security staffing duties are assigned by organizational priority and by identified risk areas or conditions. OT2-4 Security staff training paths are identified in the Security Roadmap, supporting and maintaining a relevant, vibrant, learning Company to best support the Company against known or potential threats. OT2-5 Security staff will bridge between IT and OT staffs to confirm common understanding and communications between the technical culture groups when working with modern technology security methods.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
(3) Provision for Employee Awareness and Training ***Best Practices Include*** *The Company has an acceptable use policy that outlines uses at different staff levels. The policy identifies permitted uses for:* • *Information Technology* • *Operational Technology* • *Organizational Data* • *Assets* *The Company has cybersecurity enforcement methods in place. These enable consistent company use. Methods include training, acknowledgements, monitoring and enforcement* *The Company conducts periodic cybersecurity awareness training for all staff. This enables understanding of policies, procedures, and safeguards to minimize threats.* *The Company routinely promotes cybersecurity due care and diligence. This builds cultural practices based on cybersecurity requirements.* *The Company proactively reviews organizational cybersecurity risks at the executive management level. This assesses the potential impacts of security breaches, the protective practices in place, and related employee training.*	***Process Specification Requirement*** P3-1 The Company provides, equips and executes employee cybersecurity training at initial employment to confirm indoctrination with organizational technology, systems, data, and acceptable use. P3-2 The Company provides, equips, executes and tracks results of periodic employee cybersecurity training on organizational security expectations; organizational policy, procedures and safeguards; technology threat sources; potential or actual risk topics; and methods by which threat actors may gain unauthorized access to organizational systems, personnel or data. P3-3 The Company provides training to executives and travelers to help them understand cyber-related threats and risks which they may encounter while traveling away from their home locations. P3-4 The Company develops personnel security knowledge through career development programs that proactively build employee skills to support the Company's long-term skill requirements. P3-5 The Company's protective systems are managed by security-vetted personnel who are experienced, trained, and skilled in converting monitored systems outputs into required protective actions. P3-6 The Company provides specialized training for system administrators and maintenance personnel who are considered to be "privileged users." P3-7 The Company integrates lessons learned and best practices from outside and inside activities into training to confirm the enterprise is a 'learning organization.'	***Information Technology Specification Requirements*** IT3-1 Employees receive initial cybersecurity training upon employment with the Company. This training will communicate documented OT security expectations to Company employees, contractor personnel, and supplier personnel having authorized access to the Company's OT. Training includes technology acceptable use, potential risk conditions or threats they may encounter, and their expected actions, counteractions, and reports to higher authority in these events. IT3-2 Employees receive cybersecurity training on email, messaging, web surfing and social engineering topics on a periodic basis. IT3-3 Employees receive cybersecurity safety training for home and travel, to confirm they are informed concerning threats to organizational assets and data in their homes, while traveling or while in locations not associated with the Company's known facilities or asset locations. IT3-4 Technology service employees, either in the Company's IT structure or contracted services, receive (1) standard employee training for cybersecurity topics, (2) more detailed cybersecurity training, as required, to confirm they know countermeasures and mitigating actions against the threats known or suspected to be relevant to the Company, and (3) access control (provisioning/deprovisioning) process training for cross-departmental processes that affect personnel access to IT, OT or both. IT3-5 Employees receive change management training for technology differences and impacts of new systems, applications, processes or methods when any of those may affect organizational personnel, systems, processes or data.	***Operational Technology Specification Requirements*** OT3-1 Relevant employees receive initial operational or process control system cybersecurity training upon employment with the Company. This training will communicate documented OT security expectations to Company employees, contractor personnel, and supplier personnel having authorized access to the Company's OT. Training includes technology acceptable use, potential risk conditions or threats they may encounter, and their expected actions, counteractions, and reports to higher authority in these events. OT3-2 Relevant employees receive operational or process control system cybersecurity training on a periodic basis. This material includes allowances or restrictions on conventional IT services (e.g., email, messaging, file transfer, remote access) in their interfaces with OT systems. OT3-3 Relevant employees receive operational or process control systems cybersecurity threat or risk condition training on a periodic basis, illustrating potential technical or architectural issues in the organizational OT systems, and how human errors or system flaws may cause loss of system, data or operational integrity. OT3-4 Relevant employees receive operational or process control systems cybersecurity training on potential impacts of risk conditions or threats on regulatory or compliance postures of the Company. Such training includes potential effects of cyber-enabled system intrusions or failures, and impacts on systems, assets, personnel, or environment. The training may also include, if appropriate, the potential impacts of technology issues (intrusions, failures, errors, etc.) on International Maritime Organization (IMO) or individual Flag State compliance requirements.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		IT3-6 The Company's security leadership assesses, on at least an annual basis, the tailored training requirements necessary to address changing threat or risk conditions to the Company and its employees, systems and assets, to confirm that such training is provisioned through the next budget cycle. IT3-7 The Company integrates risk assessment results to the internal employee or contractor training curriculum to educate personnel against risk behaviors in light of threats and best practices. IT3-8 The Company cross-trains cybersecurity personnel and operational technology engineers in order to encourage and maintain open communication between the two groups. IT3-9 The Company maintains a staff of experienced internal cybersecurity audit personnel who are knowledgeable of and trained in the organizational cybersecurity architecture, policies, procedures, and implementation. IT3-10 The Company provides training and awareness for social media use, cautioning against operational security issues (over-sharing about the Company, verbose or overly detailed job descriptions) and data sensitivity in and around the workplace.	OT3-5 The Company confirms OT field personnel get specific security-related training and procedural refreshers relevant to their operational environment, to include the latest vulnerability and threat-related information from all available sources. OT3-6 The Company's acceptable use polices clearly communicate tips and methods concerning cybersecurity "hygiene" to users through periodic training containing tips and methods for maintaining a well-functioning technology foundation. OT3-7 The Company develops, tests, and periodically trains staff on manual backup procedures for critical operational functions in the production flow. OT3-8 The Company cross-trains cybersecurity personnel and operational technology engineers in order to encourage and maintain open communication between the two groups.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
2- Risk Understanding and Management			
(4) Perform Risk Assessment ***Best Practices Include*** *The Company performs periodic risk assessments that promote revisit to operating assumptions regarding capabilities and systems monitoring needs.* *The Company exercises due care and due diligence concerning cybersecurity assets, risks, and protective systems, provisioning appropriate capabilities that yield protections which can be judged adequate against expected threats.* *The Company uses a construct to frame the methods and techniques required to bring all cybersecurity actions, automated systems, and risk management processes into a single management system.* *Risk management processes include risk indicators that allow effective and proactive handling of risks in decision making.*	***Process Specification Requirement*** P4-1 The Company provides and executes risk assessment events on a regular basis, with scheduling determined by (1) acquisition, integration or procurement of new systems or assets; (2) changes in potential risk posture in any systems or assets; or (3) at least an annual basis. Risk assessments include reevaluations of enterprise assumptions and requirements for internal cybersecurity capabilities and system monitoring. P4-2 The Company has identified an appropriate method for risk assessment that personnel are trained to use, that is used regularly, and which is subject to review or inspection. *P4-3* The Company specifically describes risk indicators that trigger effective and proactive risk prevention and resolution decision-making. *The Company considers both potential external and internal threats in developing its risk assessment.* P4-4 The Company provides a form of the periodic risk assessments to Company leadership for risk factor governance. P4-5 The Company conducts specific risk assessments against potential risk and threat conditions in new acquisition programs, using output to inform and shape protective systems architectures and further, more detailed lifecycle risk analyses. P4-6 Organizational leadership requires and reviews a periodic assessment of organizational security capabilities and status, including gaps in protection processes, systems, and staffing (both coverage and competencies). P4-7 The Company specifically describes risk indicators that trigger effective and proactive risk prevention and resolution decision-making.	***Information Technology Specification Requirements*** IT4-1 IT risk assessments are conducted annually, and as required by events and/or configuration changes, with (1) records of assessments, (2) action lists from assessments, and (3) residual risk lists kept for periodic review and update. IT4-2 IT risk assessments are informed by active measures in the security architecture (perimeter and interior defenses, and asset inventory and management tools) and to passive measures (log management and log data mining for security event analysis) for a holistic view of systemic risk. IT4-3 IT risk assessments are provided as inputs to enterprise risk management processes, informing enterprise risk with technology components. IT4-4 IT risk assessments are built from the Company's Functional Description Document (FDD) or similar, and they consider the entire IT and data attack surface(s) of the enterprise in their consideration of risk assessments, estimates, mitigations, remediations and acceptances. IT4-5 IT risk assessments consider organizational assets (data, property, personnel, processes, operational methods or functions) and generate a risk profile across asset classes for organizational risk governance. IT4-6 IT risk assessments are conducted with Network Operations and Enterprise Architecture personnel as participants. IT4-7 IT risk assessments are conducted on new systems, new procurements, and new-build assets of all types, to include project development and construction factors as potential risk inputs for operational capabilities.	***Operational Technology Specification Requirements*** OT4-1 OT risk assessments are conducted annually, and as required by events and/or configuration changes, with (1) records of assessments, (2) action lists from assessments, and (3) residual risk lists kept for periodic review and update. OT4-2 OT risk assessments are built from the Company's Functional Description Document (FDD) or similar, and they consider the factors associated with networking of control systems, both positive and negative, as part of risk assessment analyses and reporting. OT4-3 OT risk assessments are reported as action-oriented requirements, meant to support remediation or mitigation actions, and to enable audit and enforcement of information system security policies. OT4-4 OT risk assessments, and most specifically those associated with operational systems with safety-related impacts, are subject to layers of decision review commensurate with the Company's enterprise risk governance and risk management processes. OT4-5 OT risk assessments of operational systems generate output in standard reporting formats for which employees are trained to use, understand and to which they can contribute. OT4-6 OT risk assessment reports are capable of standing alone as individual products, but their output can be / is used as standard inputs to more detailed risk, hazard, safety, compliance and security analysis efforts.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P4-8 The Company documents and archive the results of the risk management and risk tolerance assessment meetings and resulting risk management plans. P4-9 The Company develops and maintains an OT functional description document (FDD) containing all appropriate and relevant information concerning communications networks among functional elements of the industrial control system(s) (ICS), interfaces among ICS and non-ICS elements, and representing the functional architecture of the ICS and connecting networks. P4-10 The Company considers management of change (MoC) as a potential carrier of OT/ICS security risks and includes evaluation of supplier processes and process implementations for OT hardware, firmware and software. P4-11 The Company performs a standardized risk assessment for need-based access required for subcontractors or suppliers to facilitate authorized access to offshore or marine OT assets. P4-12 The Company uses relative risk assessments to guide and measures the internal and endpoint scanning activities across enterprise systems, devices, appliances and assets.	IT4-8 The Company uses risk assessments and report products to develop topics for employee risky behavior training, and to feed forward into organizational policy updates. IT4-9 The Company inspects all third party service providers that require access to enterprise data to confirm they meet minimum standards for security as per the Company's requirements, and that they can sustain secure operations at least during the course of the contract.	OT4-7 The Company defines and assigns roles and responsibilities required to support a baseline security risk assessments of each marine or offshore asset. Review participation in assessment team activities to determine that the personnel/organizations having knowledge of the ICS implementation aboard each asset establish risk levels of tolerance. OT4-8 System interface descriptions and inventory are maintained and kept updated to support risk and vulnerability assessment efforts. OT4-9 The Company considers and models for the possibility of cascading failure events, and establishes incident response procedures that limit or prevent significant impact of those events on linked systems, neighboring organizations, or the community. OT 4-10 The Company uses risk assessment and risk management processes to define and implement acceptable use policies and methods for use of remote access to offshore, marine or physically inaccessible OT or ICS. Risk assessment and formal decisions concerning accesses and methods comply with organizational access policies. OT4-11 The Company conducts a defined review process to periodically consider existing offshore or marine ICS risks, identify and evaluate new risks, and update corporate tolerance for risks aboard offshore or marine assets.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
(5) Provide Perimeter Defense ***Best Practices Include*** *The Company understands its networked systems and decides on protective systems based on the functions they provide, rather than the category or brand name. The functions integrate within the security Company to provide more complete knowledge of operational security.* *Tools are used by experienced, trained personnel who have the access and insight to interpret the tools' output as required actions.* *The Company screens communications paths and messaging (e.g., email or social messaging methods) prior to its delivery into the Company, or to the recipient's mailbox, to detect and remove any hazardous files, attachments, or links.* *The Company protects perimeter or protective equipment, appliances or systems against unauthorized access by use of screening mechanisms, access control lists, complex passwords and/or two-factor authentication, and out-of-band communications paths.* *The Company documents and tracks security device, appliance, and system configurations and settings, for better understanding of current configurations, periodic training for existing and new personnel, and audit capability for the equipment and systems.*	***Process Specification Requirement*** P5-1 The Company has, maintains, and uses system architecture documentation and asset inventory accounting for enterprise, system, vessel or asset security requirements, security functional needs, and security protective capabilities, and tracks such data in the Functional Description Document (FDD). P5-2 The Company uses risk assessment and risk governance processes to inform and shape the systems, data, assets, business or mission function, and personnel protective requirements to match organizational risk profiles and risk acceptance. P5-3 The Company defines security protective functions across the attack surfaces of the enterprise, including functions to screen and/or protect available, exposed, and/or vulnerable areas of the enterprise networks, as part of security architecture documentation in the FDD. P5-4 The Company defines security protective functions to address potential threats or threat sources, providing and supporting the minimum essential protective functions that can be expected to protect critical functions, data and safety-critical systems, and which can be supported within the Company. P5-5 The Company provides security automation methods and functions to security teams for data stream consolidation and use by assigned security team personnel as part of daily assigned security monitoring duties. P5-6 The Company uses security functions and systems to generate security data streams for continuous monitoring capability. P5-7 The Company uses security functions and systems to generate alerts and events which may require investigation by assigned security personnel or by the Incident Response Team (IRT).	***Information Technology Specification Requirements*** IT5-1 The Company maps networked assets to understand holdings, property, physical and digital assets, and critical functions that must be protected and maintained to support the enterprise and its work efforts, including this documentation as part of the Company's Functional Description Document. IT5-2 The Company assesses and records its IT-based attack surfaces, including interfaces to other domains (OT or cyber-physical and process control systems) to include at least • Endpoints (nodes) • Personnel • Network infrastructure • Data transmission paths • Server systems • Applications • Web (public)-facing servers / apps • Data stores and assets • Devices and process control system interfaces IT5-3 The Company centralizes security functions across its communications paths to confirm all internal, external and cross-domain communications are screened against the security functions implemented to protect enterprise assets. IT5-4 The Company decomposes protective functions in networked environments to match process, data, software and functional assurance, testing and, personnel requirements. IT5-5 Minimum and essential protective functions are reported in allocation and employment against potential threats in the Company's periodic risk assessment reports.	***Operational Technology Specification Requirements*** OT5-1 The Company maps both networked and standalone OT and process control assets to understand holdings, property, physical and digital assets, and critical functions that must be protected and maintained to support the enterprise and its work efforts, including this documentation as part of the Company's Functional Description Document. OT5-2 The Company provides isolation of logical access to OT/ICS to confirm traffic to control systems can only originate from authorized sources within the Company's environment. OT5-3 The Company limits communications to/from OT/ICS and reporting sensors or devices to confirm it is screened and filtered from outside connectivity (i.e., direct Internet connection) by proxy services and appropriate firewalling and other protective services as required by relative risk. OT5-4 The Company requires IT-OT interface systems and protocol converters to be physically protected from unauthorized access. OT5-5 IT-OT gateway or interface systems are limited to strictly regulated ports, protocols and services (PPS); ordinary network functions are not allowed to remove common possible threat vectors; email, web browsing, and common utilities (FTP, telnet, etc.) OT5-6 IT-OT gateway or interface systems are maintained under strict file transfer controls and screening OT5-7 OT/ICS are regulated for allowable and allowed software and services that is allowed to run on the systems. OT5-8 OT/ICS are configuration-controlled for PPS and periodically scanned for PPS compliance and configuration hardening.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P5-8 Outside best practices, lessons learned and threat information is provided by the Company to confirm security protective functions are adjusted or managed as required to protect against new threat and attack methods. P5-9 The Company matches enterprise application and functional appliance portfolio systems against ports, protocols and services (PPS) allowed through the system architecture, adjusting PPS allowances through protective systems based on risk assessments of specific systems needs balanced against relative risks and known threats in those PPS spaces. P5-10 The Company highlights and prioritizes protective functions associated with compliance systems or Flag State compliance requirements to confirm they are specifically monitored and auditable under the security program. P5-11 The Company routinely reviews protective mechanisms and controls in place around safety-critical and mission-critical systems, ensuring no configuration or management changes can occur to such critical systems without required approvals, rigorous testing, and documentation updates to the FDD. P5-12 The Company matches security staffing against protective systems to confirm personnel skills and experience coverage on all critical protective systems. P5-13 The Company uses operational assets to provide training for security personnel, in a contextually-sensitive environment to accelerate potential learning and experience. P5-14 The Company requires safety-critical systems that cannot be effectively screened from threats to have manual or out-of-band backup systems to confirm that loss of single systems cannot result in human, environmental or ship/platform safety issues.	IT5-6 The Company places new systems, appliances, devices, applications or servers on the main network only after testing has shown the system under test to provide no functional or security hazard to the network on which it will be resident. IT5-7 The Company maintains a protective system rules log for security system function management and traffic understanding, performing regular audits to confirm compliance with plans and assets. . IT5-8 The Company tracks ports, protocols and services (PPS) required by enterprise assets and maintains a record of system rules or allowances for specific purposes (systems, appliances, devices, applications, servers, etc.), with all other PPS denied, limited or deactivated at perimeter devices. IT5-9 The Company maintains records of protective system configurations, access allowances, setup scripts, safeguarding and enforcing configuration management across all security systems. IT5-10 The Company segregates control channels and account accesses to protective systems through out-of-band communications methods to the systems or devices; communications may be by segregated Virtual Local Area Network (VLAN) if provisioned with strict limitations on access. IT5-11 The Company performs end-to-end security system (security stack) testing to confirm security systems have visibility over assets and traffic streams as intended or expected. IT5-12 The Company provides host-based intrusion detection services on servers that do not have continuous monitoring organizations in their normal process stacks.	OT5-9 OT/ICS and reporting devices are configured to limit their communications and data reporting to protected systems; built-in web servers or web interfaces to data reports are tightly controlled, with limited and monitored access. OT5-10 OT/ICS and reporting devices are connected to a protected network segment with limited, delineated access methods and protocols for both operators and other communicating machines. OT5-11 OT/ICS communications paths provide full Secure Socket Layer / Transport Layer Security (SSL/TLS) inspection capability (on perimeter and proxy devices). OT5-12 The Company makes specific allowances for safety-critical or operationally-critical systems to be scanned for malware or IoC through manual methods, thereby to avoid automated scans causing potential interruptions of service while performing critical functions. OT5-13 Reporting devices, especially those that cannot be readily accessed or updated, connect to their network receptors in ways that strictly filter their communications to exclusively the data they are meant to report, and control signals for the devices, to avoid inadvertent access to the network through overly broad applications programming interfaces.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P5-15 The Company requires irregular but frequent internal scans of systems, devices, appliances, servers and assets for malware or indicators of compromise (IoC), based on threats and relative risk conditions. P5-16 The Company uses perimeter devices to monitor for prohibited behaviors and actions (e.g., using offboard cloud resources that are prohibited by policy), reporting such compliance violations as required. P5-17 The Company monitors and regularly updates its endpoint and server scanning software utilities (antivirus, anti-malware, or anti-spyware).	IT5-13 The Company monitors inter-domain interfaces (IT-OT or OT-IT) for any traffic types, protocols, or amounts of traffic inconsistent with operational needs, blocking any PPS or traffic found not to directly correlate to enterprise portfolio assets. IT5-14 Traffic through all messaging systems (email, text exchanges, service messaging, Internet Protocol message methods, and others as required) is screened and cleaned prior to delivery to recipients, providing stripping services and screening against junk email (spam), hazardous attachments and links, and document macros. IT5-15 All hypertext transfer protocol (http or web) traffic routes through web reputation filtering and Domain Name Service filtering prior to reaching open Internet address spaces, and said reputation filtering provides protective functions for web browsers against potential malware downloads or webpage-based endpoint browser intrusions. IT5-16 The Company confirms all devices, appliances, systems, or applications are checked and proofed against default credentials or passwords prior to their being placed in the network environment; any system with hard-coded credentials shall be disallowed from being placed online in the enterprise network. IT5-17 Gateway systems, interfaces or protocol converters between IT and OT systems shall be provided as headless single-purpose systems, as much as possible, with minimal interfaces, and no standard services or ports that would allow their use for ordinary purposes (email, messaging, etc.) IT5-18 Protective traffic screening and filtering systems (firewalls or Unified Threat Management devices) are installed and maintained in a ‘default deny’ status, with exceptions allowed for permitted traffic and PPS.	

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		IT5-19 Protective systems, infrastructure devices and servers may be enumerated from within the network by authorized, specified addresses and applications or systems, but not by any other means, and especially not from external addresses or unauthorized applications. IT5-20 The public-facing address space of the network is proxy-shielded from the private address space of the network, with no protocols or related queries (e.g., ICMP), and no address crawlers able to penetrate the private address space without specific allowance at the perimeter screening devices. IT5-21 Directories and directory structures are shielded from outside query, and internal protocols and configurations are set to prevent address spoofing (e.g., ARP poisoning) which could cause internal information to be compromised to an intruder. IT5-22 Mobile device connections to the network are screened through the enterprise security stack to confirm cross-domain malware cannot penetrate networked systems without either detection or communications defeat. IT5-23 Command-line utilities such as PowerShell are tracked by interior defensive services to alert as part of Incident Response and Recovery as necessary. IT5-24 The Company provides egress filtering through perimeter devices and behavioral analysis systems, providing alerts on data or enterprise assets being accessed or moved by unorthodox or unauthorized means. IT5-25 The Company monitors web servers, both internal and external, for unauthorized access or commands, or for potential intrusion, especially in the case of web servers for which exceptions to allowable ports, protocols or services have been made.	

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
(6) Prepare for Incident Response and Recovery ***Best Practices Include*** *The Company has an Incident Response Plan (IRP) that incorporates:* • *Lessons learned from previous episodes and events;* • *Notification lists for those personnel needed to understand the incident, or to take part in the response to it;* • *Communications plan for internal personnel that provides continued operations while dispelling fear;* • *Communications plan for external agencies and personnel to maintain the organizational perspective;* • *Control plan for hazards that may affect personnel or systems;* • *Control plan for hazards that may expand beyond the Company's boundaries into the surrounding environment (i.e., affect neighbors or otherwise foment liability); and* • *Recovery plan for establishing a known set of conditions, consolidating those conditions for safety of personnel, systems, ship/platform/facility, and environment, and moving back to full operational capabilities.* *The Company conducts periodic and cyber incident drills that rehearse actions and reactions employed to recognize, control, and recover from a cybersecurity event that affects critical systems, data, and functions.*	***Process Specification Requirement*** P6-1 The Company provides an Incident Response Plan (IRP) to define roles, responsibilities, immediate actions, subsequent actions, space and equipment requirements, and recovery needs for organizational personnel, thereby establishing a uniform method for identifying, designating, and responding to an IT or OT incident. P6-2 The Company uses lessons learned from previous security incidents and events to improve and measure IRP content, and Incident Response Team (IRT) tactics, techniques and procedures. P6-3 The Company appoints and maintains an Incident Response Team (IRT) to act on indicators and events under the IRP, and those other occasions as required or directed. P6-4 The Company conducts periodic Incident Response Team training to confirm familiarity with procedures, efficiency of communications, and effectiveness of control and recovery procedures. P6-5 The Company requires all reporting-capable or logging-capable devices to provide data logs or streams to a secure, central collection repository that can be used by the IRT when investigating, controlling or recovering from an event. P6-6 The Company maintains out-of-band communications methods that allow private communications of Incident Response and Recovery (IR&R) information (plans, activities, threats, intrusion data sets, etc.) separate from the enterprise network paths. P6-7 For each safety-critical or mission-critical system IT/OT/ICS, the Company documents hazard control, environmental and safety concerns and actions, restoration and recovery activities, backup activities (e.g., frequency and safe storage), test activities, and communication plan for both responders and non-responders.	***Information Technology Specification Requirements*** IT6-1 The Company compiles anomalies and exceptions from its normal protective system data stream reporting, matching threat information against reported events to determine response requirements. IT6-2 Attack response protocols include: (1) Integrated tools and methods for identifying the type of attack; (2) Identify malware from logs; (3) Restore mission-critical systems from secure backups, and scan restored systems for functionality; (4) Monitor accounts and devices found to be related to the attack, and isolate them to prevent recurrence; (5) Force a network-wide password reset for local hosts, disallowing remote changes, and including administrators or privileged accounts, normal user accounts, and machine accounts; (6) Consider third parties that must be notified, or which can assist in investigation and recovery. IT6-3 The Company provides backup data sets and backup application software for workstations (nodes), servers, databases, safety-critical applications or systems, mission-critical applications or systems, and any other appliances, systems, devices or applications deemed necessary to the safe operation of the enterprise and its assets, in accordance with the organizational risk assessment. IT6-4 Backup data sets are at least single-redundant, maintained in secure locations segmented away from the main network(s), and kept under limited access.	***Operational Technology Specification Requirements*** OT6-1 The Company establishes a uniform method for identifying, designating, and responding to an OT/ICS incident. OT6-2 The Company considers and models for the possibility of cascading failure events, and establishes incident response procedures that limit or prevent significant impact of those events on linked systems, neighboring organizations, or the community. OT6-3 The Company establishes and maintains a coordinated onshore and offshore or marine ICS security incident response capability, to include the organizational roles, responsibilities, and staffing requirements for assuring an appropriate and timely response to an ICS security incident, including the designation of an ICS Security Incident Response Team (IRT) for each offshore or marine Asset. OT6-4 The Company actively maintains an OT Recovery Action Plan (RAP) as part of the IRP to reestablish normal safe operating conditions for the impacted personnel, systems, ship/platform/facility, including a plan for recovery from any detrimental environmental impacts. OT6-5 The Company has an Incident Response and Continuity Plan (IRCP) that contains notification lists and processes for communicating with incident responders. OT6-6 The Company maintains and protects out-of-band communications that allow control and access to OT/ICS through separate communications than enterprise network paths. OT6-7 The Company uses fault or failure modes documented in the Functional Description Document (FDD), system diagrams and log records to differentiate between system casualties and cyber intrusion events.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P6-8 The Company has known-safe conditions for IT and for OT/ICS that are documented and trained in case system operations must be configured for isolation in safety or operational recovery modes. P6-9 The Company conducts periodic reviews and updates for the software that supports incident response activities for both IT and OT incident detection and control.	IT6-5 The Company keeps backup application software copies available in safe storage for mobile units (ships) that have limited bandwidth, in case of restoral needs while away from port. Backup software copies and license keys are stored in secure segments on the network, or in secure physical storage with limited personnel access. IT6-6 Vulnerabilities found in the course of either incident response procedures audit, or during actual incident response and recovery activities, are fed forward to process personnel responsible for configuration and patch management. IT6-7 The Company conducts and documents non-periodic reviews of IT security incident detection technologies and processes. IT6-8 The Company establishes a process for improving the performance of incident detection processes, correcting shortfalls in performance of detection processes and technology, and for improving related execution of the corporate IT security and risk management program. IT6-9 The Company includes enterprise-wide certificate management as a contingency procedure in its Incident Response Plan, in event of a Certificate Authority or encryption algorithm compromise.	OT6-8 The Company establishes target metrics for ICS performance and monitor that performance; reports performance variances that indicate possible or actual security breach attempts; records and reports variances as indicators for needed analysis of anomalous ICS performance; and determines if the variance indicates a possible or actual security breach ("incident"), documenting the determination. OT6-9 The Company establishes and documents an incident response and continuity plan for each ICS function by incident level of severity per incident type, including restoration and recovery activities, backup activities (e.g., frequency and safe storage), test activities, and communication plan. OT6-10 The Company will respond to each incident based type, severity, and the response protocol established by the approved incident response and continuity plan. OT6-11 Attack response protocols include: (1) Tools and methods for identifying the type of attack, and regaining positive control of operational systems; (2) Disable all remote (including RDP & VPN) access until complete password change has been effected; (3) Control any safety-related or environmental impacts; (4) Restore mission-critical systems from secure backup operational software, and test restored systems for functionality; **(5)** Consider third parties that must be notified, or which can assist in investigation and recovery.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
			OT6-12 The Company documents and reports all ICS security incidents by occurrence, severity, and type, including description of impacts, (experienced and potential) with respect to safety, environment, production, lost-time, and cost (actual or anticipated if known), incident recovery measures and post-incident remediation impacts if any. OT6-13 The Company periodically employs a security evaluation tool and defined process to determine its overall security status, to identify security coverage gaps, and to define new requirements for security system improvement. The tool are also useful for performing an IRCP performance audit and update, including lessons learned when available. OT6-14 Vulnerabilities found in the course of either incident response procedures audit, or during actual incident response and recovery activities, are fed forward to process personnel responsible for configuration and patch management. OT 6-15 The Company conducts and documents periodic reviews of ICS security incident detection technologies and processes. OT 6-16 The Company establishes a process for improving the performance of incident detection processes, correcting shortfalls in performance of detection processes and technology, and for improving related execution of the corporate ICS security and risk management program.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
3- Protected Resources and Accesses			
(7) Provide Physical Security ***Best Practices Include*** *The Company provides security and securing methods for all computational equipment that controls aspects of safety-related operations, or interfaces to systems that control aspects of safety-related operations.* *The Company keeps physical security sensor feeds and system connections logically separate from production network content, segregating physical security system data flows to prevent either casual snooping or inadvertent interference within the normal scope of network operations.* *The Company confirms all computationally-enabled physical security equipment (cameras, sensors, electronic locks, networked accesses, etc.) have passwords that are (1) changed from default; and (2) non-trivial and cryptologically strong.* *The Company has considered risks associated with computationally-enabled physical security equipment so that inadvertent login failures and/or lockouts, loss of power, reboot events, and the like will not impact safety-critical operations.* *The Company safeguards its systems and device infrastructure with physical security and other means to limit access to critical equipment or safety-related equipment to authorized personnel, `with appropriate accesses and means, only.* *The Company regularly tests physical and environmental control and security sensors, devices, systems, appliances and applications, in accordance with both manufacturer and owner direction or guidance, to keep these systems in peak, known operational states.*	***Process Specification Requirement*** P7-1 The Company provides traceable physical security and access mechanisms, with logging and reporting for the systems, for sensitive or critical system spaces, assets or facilities. P7-2 The Company provides physical security for all automated or computerized systems, software or discrete assets, and especially for those that control or interface with safety-related operations or systems. P7-3 The Company routinely tests the functionality of physical access control devices and applications as recommended by the manufacturer and/or internal security policy or guidelines. PT7-4 The Company confirms that no critical system communications lines, systems, appliances or devices are left unprotected and exposed if physical attack against those components could disable mission-critical or safety-critical systems. PT7-5 The Company confirms that all critical system communications lines, systems, appliances or devices are fault tolerant and redundant as required for resilience against physical damage to prevent disablement of mission-critical or safety-critical systems. P7-6 The Company treats physical intrusions against protected cyber-physical systems, or against mission-critical or safety-critical systems, as reportable incidents to be addressed by Incident Response Team protocols. P7-8 The Company governs portable data storage through publicized standards and policies, and it provides safe storage and access limitations on any data or asset storage methods that could be lost, stolen, or target of espionage.	***Information Technology Specification Requirements*** IT7-1 The Company provides traceable physical security and access mechanisms, with logging and reporting for the systems, for sensitive or critical system spaces or facilities. IT7-2 The Company provides security for technology assets in all spaces and locations, using both security controls and responsibility assignments to prevent physical loss of assets. IT7-3 The Company provides specific physical access security to those assets with digital access to critical data, or to mission-critical or safety-critical systems. IT7-4 The Company provides physical access security to network and networking infrastructure devices to prevent tampering, theft or secret replacement of trusted devices. IT7-5 The Company provides separate logical network connections (Virtual Local Area Networks (VLANs)) with specified access control lists (ACLs) for physical security monitoring and surveillance devices and systems, and for access control systems on critical spaces or facilities. IT7-6 The Company confirms any physical security access or surveillance systems are maintained under security separate from other IT assets, with separate password and administrative access in accordance with separation of duties. IT7-7 The Company confirms any physical security access or surveillance systems have access accounts and passwords changed at system installation and at intervals determined by the Company in accordance with due care and due diligence.	***Operational Technology Specification Requirements*** OT7-1 The Company establishes and maintains physical security procedures that complement OT/ICS software security policies and fully leverage physical access control as a first-level ICS security measure. OT7-2 The Company provides traceable physical security and access mechanisms, with logging and reporting for the systems, for sensitive or critical system spaces or facilities that house or host OT/ICS. OT7-3 The Company provides security for OT/ICS assets in all spaces and locations, using security controls, securing devices (locks, cables, seals, etc.) and responsibility assignments to prevent physical loss or tampering of assets. OT7-4 The Company provides specific physical access security to those assets with digital access to critical organizational cyber-physical functions, or to mission-critical or safety-critical systems. OT7-5 The Company protects the computer infrastructure that supports critical equipment control and safety-related control from unauthorized physical access, to include at least all IT-OT interface systems and protocol converters. OT7-6 The Company isolates process control systems or OT/ICS from general-purpose computing systems to remove potential cross-system human errors or corruption of OT/ICS from ordinary computing systems. OT7-7 The Company provides physical surveillance of mission-critical or safety-critical systems, with similar surveillance and tracking for systems, appliances or avenues of access that provide critical functions or inputs in support of mission-critical or safety-critical systems.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		IT7-8 The Company develops and applies procedures and methods for mission-critical and safety-critical systems (i.e., Integrity Level 3) that will prevent unsafe conditions in case of inadvertent login failures, user lockouts, power loss, or reboot events. IT7-9 The Company provides safe storage for important IT assets, such as encryption certificates, physical access keys and combinations, software original media, enterprise 'gold disk' builds and media, etc., that is proof against intrusion and reasonable expectations of environmental threats. IT7-10 The Company provides safe storage for operational data to prevent any but authorized access, and to protect it from environmental hazards.	OT7-8 The Company provides physically-protected, fault-tolerant power to mission-critical or safety-critical systems that are judged IL3 criticality to the ship or asset and its personnel. OT7-9 The Company confirms that physical security equipment that is linked or linkable to computer networks remains operational and unaffected by power loss, software reboot, login failures, and/or system lockout. OT7-10 The Company provides safe storage for operational control system data to prevent unauthorized access, and to protect it from environmental hazards.
(8) Execute Access Management ***Best Practices Include*** *The Company screens personnel for security issues prior to onboarding.* *The Company allows no group login credentials, and shared credentials/sharing of credentials are prohibited.* *The Company requires two-factor authentication to access sensitive resources or assets, or to access networked assets remotely.* *The Company periodically inventories third-party access and relationships to confirm that all network and/or data access are current, required, and under governance and control.* *The Company requires authorized third-party personnel with access to organizational networked systems to use two-factor authentication for connection, or strong passwords that cannot be easily guessed.*	***Process Specification Requirement*** P8-1 Personnel access to systems, data or enterprise functions is granted on the basis of least privilege, need to know and minimum access required to fulfill role requirements (least functionality). P8-2 Machine or system access to networked systems, data, personnel or enterprise functions is granted on the basis of functional requirement for connection, least privilege, minimum required access, and continuous performance and security monitoring. P8-3 The Company uses personnel vetting processes for employees, contractors and consultants to confirm trust can be established on the basis of known factors and conscious decisions. P8-4 The Company uses well-defined processes for vetting third-party personnel and computers that are credentialed for access to proprietary networked resources.	***Information Technology Specification Requirements*** IT8-1 The Company requires positive confirmation of need to know and role-related requirements prior to granting access to enterprise data in any form, and especially prior to granting access to shared repository assets. IT8-2 The Company positively tracks personnel, role or job, and system, functional or data access responsibilities to confirm clear responsibilities, authorities and accountability exist across all technology areas in the enterprise, for both technology administrators and technicians, and for enterprise employees in other departments. IT8-3 The Company confirms all personnel are trained and aware of their responsibilities and accountability to keep positive control of their system and data access methods, credentials and certificates to confirm insider attacks cannot be hidden under legitimate username accesses.	***Operational Technology Specification Requirements*** OT8-1 The Company safeguards data about the OT/ICS and limits access to system technical data to authorized personnel. OT8-2 The Company defines and implements role-based business rules for logical access to the ICS; access authorization within those rules is based on job function requirements and risk assessment processes, and the rules specify those systems or portions of control systems to which access is granted, per role. OT8-3 The Company lists the various user roles based on a segregation of duties (e.g., User, Maintenance, Administrative, etc.) for each major ICS functional system, including the level of functionality permitted for each role based on job responsibilities and risk analysis. OT8-4 The Company implements a formal enrollment process that verifies the identities of persons, machines and software authorized to access the ICS, and specifies those systems or portions of control systems to which access is granted.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company has defined, and uses, a third-party supplier program, including supplier vetting prior to granting access to networked resources. *The Company requires all remote access users to pass through security and authentication systems to provide traceability of communications and tracking or logging of actions carried out remotely. No remote access can occur without strict accountability for all communications.* *The Company limits privileged access accounts to those identified personnel with specific work-related needs.* *The Company limits privileged accounts to specific systems and does not allow those accounts Internet access (outside access is limited to non-privileged accounts).* *The Company requires login credentials for users to access guest wireless network resources, to provide usage tracking as necessary.* *The Company implements login failure time-out periods to prevent password guessing.* *The Company decides single sign-on (SSO) boundaries on the basis of data or application criticality, leaving certain designated applications, systems, repositories or functions outside SSO to meter access based on separate authentication for traceability and accountability.* *The Company removes access privileges from former employees promptly so that there are no unauthorized accesses to a former employee account after changing employment.*	P8-5 The Company tracks operational or process control assets that do not have either physical or logical access control mechanisms, substituting access process controls as required to confirm positive knowledge of personnel or machine access to control systems or components. P8-6 The Company maintains positive and continuous control of mission-critical or safety-critical systems that, for reasons of timely response and/or safety, use group logins; manual watch logs and personnel tracking are required to correlate personnel against groups on watch. P8-7 The Company requires two-factor or multi-factor authentication for administrative privilege login to mission-critical, safety-critical or interface systems. P8-8 The Company requires two-factor or multi-factor authentication for any remote access to control systems, remote sensors or devices, or to administrative interfaces for remote systems. P8-9 The Company separates privileged accounts from ordinary accounts, removing all general purpose services, applications and outside access from privileged accounts to minimize the potential for personnel errors while in administrative access modes. P8-10 The Company enforces login failure limits and time-out periods to prevent brute-force login attempts against both IT and OT systems. P8-11 The Company provides or limits single sign-on (SSO) credentials and services based on specific work-related needs and security criteria identified in its security architecture (e.g., reference model, framework, or logical construct).	IT8-4 The Company logs user accesses to network resources, either local or remote, to provide accountability for each user in the network environment. IT8-5 The Company maintains a counter-insider program that logs working hours, network resource accesses, access geolocation (if applicable), and access to specified resources (critical data). IT8-6 The Company requires supervisors to confirm adequate separation of duties is maintained to guard against conflict of interest and possible insider data theft. IT8-7 The Company requires all IT privileged accounts to be managed with centralized visibility, logging and monitoring. IT8-8 The Company uses technical means (e.g., complex passwords, password escrow, two-person control) to manage privileged credentials on all enterprise or server systems. IT8-9 The Company requires administrator personnel to use ordinary, unprivileged accounts for all business functions not associated with administering systems, and for them to use privileged accounts only when performing administrator functions. IT8-10 The Company does not allow local administrator access on endpoint systems (e.g., PCs or laptops) to prevent intruders from moving laterally across networked systems. IT8-11 The Company disables unused Ethernet network ports at the enterprise switch ports to prevent unauthorized access to the network. IT8-12 The Company disallows any but named, role-based, need-to-know access to infrastructure devices and systems such as domain controllers, routing and switching infrastructure, global directories, etc.	OT8-5 The Company document the qualifications, credentials, and employee status required for authorized access to each designated ICS access point. OT8-6 The Company uses risk assessment and risk management processes to define, implement and enforce acceptable use policies and methods for use of remote access to offshore, marine or physically inaccessible OT or ICS; the formal decisions concerning accesses and methods comply with organizational access policies. OT8-7 The Company provides positive management to manage a need-based subcontractor access program to facilitate authorized access to offshore or marine ICS assets. OT8-8 The Company requires dynamic two-factor authentication (i.e., no static passwords or stored two-factor credentials) for both local and remote access to role-based OT/ICS accounts, resources or assets, implemented and enforced for employees and authorized third parties; unauthenticated access to any ICS function is strictly disallowed. OT8-9 The Company specifically disallows use of single-sign on (SSO) or stored credentials for access to OT/ICS, or to interface systems that access OT/ICS. OT8-10 The Company conducts a periodic formal risk assessment of the method for establishing and allowing remote access into each remotely accessible major ICS functional component, listing the allowable functions permitted through remote access (e.g. read-only, equipment control, configuration modification, etc.), and establishing qualifications, credentials, and employee (or server) status required for granting human user (or server) remote access to any ICS.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P8-12 The Company defines and operates with processes that link technology access administration with Human Resources to automate employee provisioning and deprovisioning to the greatest possible extent without introducing errors. P8-13 The Company defines conditions requiring separation of duties in access to technology, process control, data, test and software development areas, ensuring no single individual can achieve unintended access levels and privileges that could hazard the Company or its systems. P8-14 The Company may terminate wireless network operation during non-working hours to prevent potential unauthorized connectivity in those periods of minimal supervision and monitoring. P8-15 The Company confirms all infrastructure systems, devices or appliances, e.g., wired or wireless routers and switches, are centrally manageable and monitorable, and that they are configured in accordance with enterprise policy for password and personnel access to prevent accesses. P8-16 The Company identifies a local (onboard) authority to approve, authorize and monitor any remote access to control systems of any type, which may result in the remote control of onboard equipment or systems, especially safety-critical or mission-critical systems. P8-17 The Company considers or uses two-person control procedures for managing access to the most critical assets, or to manage mission-critical or safety-critical systems. P8-18 The Company consider hybrid logical-physical access methods or restrictions, including keypad or passphrases combined with physical tokens or keys, for especially critical data or system access.	IT8-13 The Company requires all enterprise projects to provide access requirements and restrictions that strictly segregate projects and duties within the Company until such time as the fully-developed project is ready for deployment into the enterprise environment with standard access protocols. IT8-14 The Company limits simultaneous logins from the same employee on different machines into the network based on enterprise risk assessment, but strictly disallowing geographic differences between multiple logins to prevent use of stolen credentials. IT8-15 The Company uses technical means to confirm individual endpoints can connect to only one network at a time, i.e., either wired or wireless but not both, to prevent unauthorized cross-network lateral movements. IT8-16 The Company uses risk assessment of assets and data to derive policy and technical enforcement methods for access to external cloud-based services and data storage utilities. IT8-17 The Company uses risk assessment of personnel, assets and data to provide methods of safe storage for the enterprise's most critical assets, implementing ACLs and tracked access in regular logging and reporting. IT8-18 The Company requires periodic inventory of the user base, both human and non-human entities, to confirm directory entry and username tracking for accountability are accurate.	OT8-11 The Company identifies a qualified local onboard authority to approve and monitor any remote access that may result in the remote control of onboard ICS equipment. OT8-12 The Company requires that all remote access users access proprietary networks through credential authentication systems that trace, track, and/or log their activities. OT8-13 The Company will use the same remote access and authentication methods for employees as for third parties with authorized access. OT8-14 The Company configures remote access for secure operations, implementing traceability of access and logging of all operations and actions. This includes (1) Defining the method or type of access to be used for each OT/ICS, specifying for machine or human access, classified by local/physical, local/logical, or remote/logical. (2) Removing all remote access methods or mechanisms except those which the Company will specifically allow and support; (3) Use of 'monitor only' access for any operational systems that must be monitored but not directly controlled (especially important for OT/ICS without in-system access controls); (4) Refusal of persistent vendor or third-party access connections into the OT/ICS network or its interfacing systems; (5) Requirement for all OT/ICS remote access to be time-limited, under positive operator control, logged for access and activity, and under governance of tag-out procedures.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P8-19 The Company uses an OT/ICS Security Office to review risk assessments and to approve implementation plans, controls and authorized user lists. P8-20 The Company removes access privileges from former employees promptly so that there are no unauthorized accesses to a former employee account after changing employment.		OT8-15 The Company describes and documents the OT/ICS processes and controls that will be used to protect the operational systems during remote access, and establishes the security requirements for remote devices (e.g. anti-virus, firewall, simultaneous connections, etc.) and installations (e.g. secure facility) to be required to support operational system access. OT8-16 The Company requires that any devices, systems, appliances, applications or software processes authorized and approved for remote access to any OT/ICS meet organizational policies for security, including pre-use testing. OT8-17 The Company prohibits use of portable writable drives for software transfers to OT/ICS, unless Company-owned, encrypted and scanned prior to use.
(9) Maintain Asset Management ***Best Practices Include*** *The Company tracks its working technology assets and data as the critical enablers of the business or mission, protecting them logically as well as physically, to prevent unauthorized disclosures or losses.* *The Company identifies and tracks critical infrastructure, both in physical assets and in functions, which require protection to safeguard the business or mission.* *The Company requires authorized third-party personnel and their systems to be vetted, screened, and authorized prior to connection to the Company's networked systems.* *The Company tracks and manages the obsolete equipment and related software in operational systems, keeping awareness of vulnerabilities and exposures to communications paths that could allow unauthorized access to those assets.*	***Process Specification Requirement*** P9-1 The Company actively tracks, manages and monitors network access by its authorized and inventoried endpoints, servers, appliances and devices. P9-2 The Company actively tracks and monitors the software applications authorized to be run within the enterprise, taking steps to identify and disallow use of any unauthorized software. P9-3 The Company tracks and manages software licenses as enterprise assets. P9-4 The Company confirms that all servers, endpoints, peripherals and attached sensors or devices are configured for minimum services prior to being placed on the network, per established baseline standards. P9-5 The Company strictly limits access to infrastructure and functional assets, such as servers, routing and switching, and process control systems, to authorized and trained personnel on specific access control lists (ACLs).	***Information Technology Specification Requirements*** IT9-1 The Company uses systems and technical methods to manage actively all authorized IT systems, devices, or appliances that connect to the network(s), either wired or wireless. IT9-2 The Company uses systems and technical methods to manage actively all authorized IT applications, both networked and standalone, within the enterprise, for license, usage and unwanted program management. IT9-3 The Company monitors and, when appropriate, controls all web browsing to websites outside the enterprise boundaries. IT9-4 The Company uses whole-disk (device) encryption on computational system (desktop or laptop) storage drives and/or local storage. IT9-5 The Company uses remote disablement software to neutralize corporate data or software on lost or stolen devices.	***Operational Technology Specification Requirements*** OT9-1 The Company develops and maintains a current (updated) Industrial Control System Functional Description Document (FDD) describing the ICS equipment and control system architecture for each protected asset, and including descriptions of the industrial security management functionality, system device implementation, and network implementation architecture for each asset. OT9-2 The Company identifies the physical and functional mission-critical or safety-critical OT assets that must be protected in order to safeguard employees, customers, suppliers, the corporate mission, the environment, and the public interest, and to protect the enterprise from operational disruption or operations interruption. OT9-3 The Company uses the FDD to track software inventory and software and firmware versions or requirements for each OT/ICS asset.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company actively manages open resources such as guest wireless networks, requiring passwords for authorized users, system tracking (by address and/or port), and standards for acceptable use.	P9-6 The Company positively controls remote access to any and all enterprise assets (data, machines, cloud resources, mission functions). P9-7 The Company conducts periodic asset scans across the various networks to inventory network participants, systems and devices, and authorized or unauthorized machines on the networks. P9-8 The Company tracks and manages all networked devices and systems that run on network infrastructure, but which may not be strictly IT or OT, including (but not limited to) physical security devices and systems, voice over Internet protocol (VoIP) systems, teleconference systems, video or data stream generators, sensors and reporting devices, entertainments systems, satellite communications feeds, etc.	IT9-6 The Company specifies the allowable or approved remote access software, methods and personnel or roles allowed to access network assets from locations external to the network. IT9-7 The Company specifies the allowable or approved remote access software, methods and personnel or roles allowed to conduct remote access operations to specific systems; remote access is allowed only when time-bounded and under the positive control of an internal employee.	OT 9-4 The Company protects against unauthorized logical access to proprietary operational and protective systems using mixtures of logical and physical methods, including (but not limited to) segregated communications paths, screening mechanisms, access control processes, strong passwords, and/or multifactor authentication. OT9-5 The Company references the FDD software inventory for ICS evolution control, system maintenance, personnel training, supplier management, and periodic ICS internal and regulatory audits. OT9-6 The Company tracks and manages obsolete equipment and software assets to reduce or eliminate vulnerabilities presented by unauthorized access to and the use of those assets. OT9-7 The Company confirms that all web data traffic inside the OT/ICS is completely contained within the perimeter of the operational system, and that it is available only to authorized users within that perimeter.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
CS2: Developed Capability Specification			
1- Practices, Programs, and Processes			
(10) Perform Policy Management ***Best Practices Include*** *The Company tailors security policies to its specific context, environment, and compliance needs, to satisfy useful purpose as well as meeting regulatory and reporting needs.* *The Company's policies and procedures align with its chosen standards (See Subsection 11 below) for policy positions that directly support organizational goals for technology, use, and enforcement.* *The Company confirms that its personnel initially train on policies upon starting a new position, and that they review the enterprise policies on an assigned and regular basis.*	***Process Specification Requirement*** P10-1 The Company monitors relevant industry risk management regulations and public policy to integrate with its own policies, procedures and guidance. P10-2 The Company maintains a documented registry of pertinent regulations, policies, and reporting requirements to proactively manage full compliance in its legal and regulatory environment. P10-3 The Company regularly reviews its technology and operations bases, and it provides and maintains policies for technology areas in which enterprise-wide standard guidance will work toward Company goals. P10-4 The Company uses asset and perimeter controls to determine potential gaps in policies, providing feedback for policy development from continuous monitoring or performance monitoring data. P10-5 The Company considers total systems portfolio and functional needs in aligning budget, personnel, training, outside services and system needs, seeking balance that gives the Company the best chance for assigned and authorized personnel to operate, maintain and sustain assigned systems within resource constraints. P10-6 The Company confirms baseline or minimum security requirements are defined, trained and applied across all systems prior to placing those systems onto any network, and that those minimum security requirements are periodically checked against risk conditions or potential threats to enterprise assets.	***Information Technology Specification Requirements*** IT10-1 The Company defines and uses IT policies to align system operations with security requirements across all technology areas in the enterprise, including at least cybersecurity, data security and integrity, systems test and software integrity. IT10-2 The Company defines and uses risk and vulnerability management processes to track and revisit security vulnerabilities or security issues that remain extant in systems without either remediation or mitigation. IT10-3 The Company defines and uses IT policies to assign responsibilities and accountability for systems providing mission-critical or safety-critical functions in the enterprise. IT10-4 The Company defines reporting requirements to higher authority through IT policies in order to standardize guidance for data reporting. IT10-5 The Company requires appropriate functional and security testing of proposed software applications or new systems proposed for enterprise use, with risk assessment, prior to procurement, acquisition or deployment. IT10-6 The Company uses perimeter protective devices and systems to monitor for policy compliance and unauthorized activities in addition to fulfilling their protective purposes, with compliance violations reported to appropriate responsible officials within the enterprise. IT10-7 The Company requires documentation of every new system, device, appliance or application to be provided prior to any project or procurement completion.	***Operational Technology Specification Requirements*** OT10-1 The Company creates and implements a policy that establishes an ICS Security Office to provide operational availability and continuity, to direct implementation of ICS security, to direct ICS security activities, to coordinate and direct onshore and offshore ICS security incident response capability, and to administer the CMS aboard each offshore or marine asset. OT10-2 The ICS Security Office defines and uses risk and vulnerability management processes to track and revisit security vulnerabilities or security issues in process control or OT/ICS that remain extant in systems without either remediation or mitigation. OT10-3 The ICS Security Office defines and uses OT/ICS policies to assign responsibilities and accountability for systems providing mission-critical or safety-critical functions in the enterprise. OT10-4 The Company confirms subcontractor change management practices in compliance organizational or Company software management of change (SMOC) policy and procedures. OT10-5 The Company addresses policies and procedures for control system security governance in the Functional Description Document, and in the ICS Security Office policies and procedures, ensuring no control systems are left without policy or guidance. OT10-6 The Company prohibits connections of any unauthorized type to OT/ICS as part of ICS Security Office policy.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P10-7 The Company confirms security installation and configuration technical review prior to completing major system modifications or configuration upgrades or changes, especially when third parties are involved in engineering, installation or system checkout P10-8 The Company confirms that all new projects and all new systems, devices, appliances, servers and/or applications are security tested prior to deployment on operational networks. P10-9 The Company requires documentation as a deliverable from every system development, installation, or deployment, and enterprise personnel will confirm the documentation meets organizational standards, and that it is used as part of the Functional Description Document as appropriate. P10-10 The Company confirms that operations, methods, policies, procedures and related knowledge are captured and recorded to maintain corporate knowledge for the continued safety and wellbeing of the enterprise.	IT10-8 The Company requires auditable functional similarity in security programs and policies between reporting units, enterprise systems, and subsidiaries within the enterprise. IT10-9 The Company develops and implements endpoint or device policies for hardware, software, cyber hygiene and authorization to gain access to the network and its resources.	
(11) Provide Standards and Guidance ***Best Practices Include*** *Cyber issues are covered by the governing body (Board of Directors, Executive Board, etc.) to focus on risks to the Company, investments required to address those risks, and personnel and staffing needed for solid programs.* *Cybersecurity information provided to the Board is of sufficient quantity and frequency to enable solid Board understanding of cybersecurity risks in the enterprise, necessary mitigation efforts, and tradeoff decisions about those risks.*	***Process Specification Requirement*** P11-1 The Company routinely provides cybersecurity information to its primary governing body to inform decisions concerning security management priorities – including but not limited to security risks, potential for loss resulting from security events, known and emerging threats, mitigation programs, regulation compliance, industry practices, internal assessment results, and pertinent public policy. P11-2 The Company defines and maintains an internal standard for documentation and system requirements documents that make up the Functional Description Document, demonstrating the standard by building and maintaining documentation of the enterprise systems.	***Information Technology Specification Requirements*** IT11-1 The Company defines reporting requirements to higher authority through IT policies in order to standardize guidance for data reporting. IT11-2 The Company defines hardening and configuration standards for endpoints (laptops, desktop machines, and portables), with measurement and validation procedures. IT11-3 The Company defines hardening and configuration standards for servers, both physical and virtual, with measurement and test procedures. IT11-4 The Company defines standards for hardening and resilience of web applications and web servers.	***Operational Technology Specification Requirements*** OT11-1 The Company maintains a documented functional description of its networked systems, and implements protective systems based on documented functional requirements (rather than the credentials or assurances of the protection provider/supplier). OT11-2 The Company's governance structure supports responsive decisions concerning cybersecurity risks, requirements, investments, and operations, and records of their decision meetings are maintained as part of the corporate record. OT11-3 The Company defines hardening and configuration standards for process control and OT/ICS to confirm defaults are removed, that control system security levels are known, and to protect OT/ICS equipment and services from unauthorized changes or contact.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company has an appointed and empowered Chief Information Security Officer (CISO) (or equivalent) whose responsibilities unify all information technology, information systems and data systems security in a single point of accountability. *The CISO's reporting structure is short and direct, giving priority to enterprise risk management and risk mitigation efforts.* *The Company has a governance structure that makes timely decisions about cybersecurity, systems and risk, balancing investments, business rules, and operations in order to minimize possible risks and maximize benefits from expenditures.*	P11-3 The Company considers management of change (MoC) as a potential carrier of OT/ICS security risks and includes evaluation of supplier processes and process implementations for OT hardware, firmware and software; therefore, the Company documents and enforces a corporate position for expected practices in supplier ICS change management. P11-4 The Company uses the overall enterprise security strategy to develop standards in support of the strategy execution. P11-5 The Company uses existing technology and process standards from standards establishment bodies where possible and applicable, but it will generate its own standards and procedural instructions as required to tailor its environment for safety, security and effectiveness. P11-6 The Company enforces a standard for new projects, programs, applications or systems that they be compatible with enterprise architecture and security architecture, that they be tested in accordance with enterprise system test requirements, and that they introduce no new vulnerabilities or weaknesses into the overall system to which they are installed or integrated.	IT11-5 The Company defines standards for project and procurement documentation requirements for retention as part of the Functional Description Document (FDD). IT11-6 The Company defines and maintains standards for infrastructure administrator qualifications, appointments, and removals. IT11-7 The Company defines and inspects to standards for any third party machine that will connect to the enterprise networks or access network assets. IT11-8 The Company documents changes to systems, with expected effects and changes to both relative risk position and security continuous monitoring requirements, through continuous interface with organizational change management processes. IT11-9 The Company defines and documents standards for new systems or projects to meet security requirements for integration into the enterprise, including limitations on mobile code, open libraries and utilities (as can be afforded), to prevent introduction of security weaknesses without adequate compensating controls.	OT11-4 The Company defines hardening and configuration standards for interface systems and protocol converter systems that connect to OT/ICS to remove any and all services and applications not necessary to the OT/ICS support tasks these systems perform. OT11-5 The Company defines performance, organizational, and security related requirements when contracting with third-party data management service providers and software applications providers. OT11-6 The Company documents changes to control systems, with expected effects and changes to relative risk position, security continuous monitoring requirements, and overall system functionality changes, through continuous interface with organizational change management processes.
(12) Provide and Guide Cybersecurity Hygiene ***Best Practices Include*** *The Company has a security strategy that directly influences and guides the technology strategy, in consonance with business or mission requirements. The security and technology strategies then inform the technology and user communities as to how they can expect to use technology to satisfy their expected duties.* *The Company does not allow default access methods, default passwords, or default system access roles to remain on operational systems once installed and configured.*	***Process Specification Requirement*** P12-1 The Company provides and expects good cybersecurity habits from personnel, staff and temporary additions to staff, encouraged by training materials, examples, reference materials, notices and warnings, and public reminders of sound and secure behavior on systems. P12-2 The Company limits administrator privileges on endpoints, devices, appliances and applications to specific personnel providing specific services during finite periods of time, ensuring that ordinary users do not have administrative privilege as a matter of course.	***Information Technology Specification Requirements*** IT12-1 The Company architecturally separates servers and applications from data repositories, ensuring separate credentials are required if outside the data-using application(s). IT12-2 The Company disables all server services on both physical and virtual servers, except what is specifically required for operations and support of the installed applications, systems or devices. IT12-3 The Company actively prevents use of tunneling tools (e.g., VPN) within the network(s); anonymizers; and proxies except as installed.	***Operational Technology Specification Requirements*** OT12-1 The Company scans all external computer disks and solid-state memory devices (e.g., thumb drives, memory sticks, portable hard disks, etc.) for malware prior to use with any OT/ICS or interfacing system. OT12-2 The Company conducts periodic reviews and updates of operational software holdings to confirm currency of all software used to detect and protect the ICS from malware.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company provides, through its acceptable use policy and periodic cybersecurity training, the user tips and methods necessary to maintain a well-functioning technology foundation, with rules and requirements made clear for the user community. *System maintainers have setup and configuration checklists, system test routines, and 'checkup' lists to help them assist users in keeping the technology environment safe and secure.*	P12-3 The Company prevents software from executing on endpoints and inside the network except when it is part of the enterprise application portfolio, and registered, inventoried and known as such (i.e., whitelisted); all other software requires special permissions to run, install or use, and it must be tested and approved prior to use. P12-4 The Company maintains wireless networks for internal, authorized users, including for machine-to-machine communications, and separate wireless networks for guest or unvetted users on the systems. P12-5 All organizationally-owned systems, devices, appliances, applications or machines connected to the enterprise networks are configured in accordance with enterprise hardening checklists that provide secure configuration guidance and support for endpoints, servers, utility systems, applications, etc. P12-6 The Company confirms that all services not directly necessary for business or mission use shall be disabled on any server, peripheral, endpoint or device. P12-7 The Company confirms that all utility systems (multi-function printers, photocopiers, scanners, etc.) installed under contract from external providers are governed per organizational data management and security guidelines, with no organizational data leaving the enterprise in third-party-owned machines without right of first refusal from the Company. P12-8 The Company promulgates policy for cryptologically-strong password strength and frequency of change. P12-9 The Company uses physical placement of infrastructure systems or devices to (1) augment security of those devices, and (2) clearly demonstrate tampering or physical access to the devices, systems or spaces.	IT12-4 The Company conducts both periodic and irregular sweeps against keyloggers, both physical and software-based, in applicable spaces, facilities and systems, and correlates any command and control-related log entries with any illicit applications or devices found. IT12-5 The Company uses anomaly detection systems to conduct sweeps against latent or unexecuted malware, or unauthorized software on systems or in file shares or data repositories. IT12-6 The Company keeps scripting languages for maintenance and systems management patched and updated per vulnerability management direction, logging all changes and updates as required. IT12-7 The Company keeps remote access methods, including secure shell (SSH), deactivated except when needed to execute administrative duties. IT12-8 The Company prohibits with policy and technical means the use of USB ports on mission-critical or safety-critical systems, or on systems that connect to mission- or safety-critical systems. IT12-9 The Company enforces cryptologically-strong passwords throughout all networked systems, using system restrictions and periodic testing against user passwords to enforce strength against brute force. IT12-10 The Company requires system users to use unique credentials on each system, with no password reuse across any systems inside the enterprise. IT12-11 The Company uses secure managed file transfer methods for transfer and retrieval.	OT12-3 The Company manages the use of wireless devices (e.g., WiFi, Bluetooth, RF, satellite, mobile phones, etc.) on or near the ICS, and implements security processes for wireless devices installed within ICS functional components. OT12-4 The Company provides defined and rigorously controlled methods and mechanisms to enable file transfers to and from OT networks, and it provides the means to monitor those transactions and enforce appropriate policies. OT12-5 The Company provides authorized locations for personal portable device connections for battery charging. OT12-6 The Company secures web interfaces to OT/ICS and data sources to confirm the ICS device or component application programming interfaces (APIs) are only available to authorized users or systems. OT12-7 The Company provides secured web browsers, with enterprise-approved add-on extensions as required, for interface to control system sensors and data reporting devices. OT12-8 The Company places special attention on keeping web browsers used within the OT/ICS perimeter updated, configuration-controlled, and strictly limited in terms of allowed domains to be accessed by the user on that system.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P12-10 The Company provides logical segmentation of network resources to require separate instances of authentication for users (intruders) attempting to traverse network resources for access to enterprise assets or functions. P12-11 The Company considers any system that has had connection to the Internet without enterprise protective functions in place to be contaminated; prior to connection to the enterprise networks, or after exposure to hostile environments (i.e., unfiltered Internet), any such system shall be scanned and cleaned of infections. P12-12 The Company configures appliances with internet connections (e.g., photocopiers, fax machines, etc.) according to architectural and functional requirements, with extensive dependence on manufacturer guidance, inherent security controls within the appliance, and network requirements. Appliances shall be configured for 'default deny'. Photocopy machines shall be configured to only communicate within the network as originators to specific addresses. Control channels and ports to copy machines or advanced printers shall be secured to the lowest possible set of available controls and accesses for maintaining effective and efficient operations. P12-13 The Company installs printers and utility devices configured with wireless services and webservers 'off'.	IT12-12 The Company uses the strongest available encryption types in wireless networks, requiring employee connections on the enterprise networks by either certificate or complex passphrase, and guest connections on the enterprise guest networks with daily-changing complex passphrase. IT12-13 The Company allows enterprise assets to connect to wired, or wireless networks, but not to both, and technical means enforce the anti-bridging requirement. IT12-14 The Company uses device digital identifiers or signatures (e.g., Media Access Control (MAC) identifier) for endpoints, servers and network-enabled devices to provide logging of access through wireless networks to enterprise resources. IT12-15 The Company uses device and user authentication and access methods on the enterprise guest networks to confirm accountability and traceability of actions when connected. IT12-16 The Company tracks network credential use by reported location of user, disabling accounts and credentials if mismatches on geolocation occur. IT12-17 The Company secures telephone instrument (VoIP) cables to the phones to confirm they cannot be used for clandestine connection to the network, and it removes VoIP phones from public or seldom-trafficked areas. IT12-18 The Company employs server monitoring agents to reduce the possibility of unauthorized activities in servers or server-controlled assets. IT12-19 The Company tests all utility devices, systems, applications, sensors, or appliances upon installation to confirm there are no unsecured interfaces, ports or services remaining for potential exploitation.	

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		IT12-20 The Company requires users to turn off machines not in use to prevent potential intrusion to machines. IT12-21 The Company prohibits remote access to data repositories and data stores when attempting to access the resources from outside the network. IT12-22 The Company prohibits remote access to cloud applications or cloud data systems if the access does not originate on an enterprise-owned machine. IT12-23 No enterprise system, whether workstations, laptops, desktops, docked mobile devices, or wireless mobile devices, shall allow auto-run of software when software is made available.	

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
2- Risk Understanding and Management			
(13) Gather and Use Threat Intelligence ***Best Practices Include*** *The Company gathers and uses threat intelligence to understand threat actors in the cyber world, their motivations and attack methods, and the potential for these threat actors to attack the Company.* *The Company uses threat intelligence to recognize and act on indicators of attack to improve incident response reaction times.* *The Company uses threat intelligence about potential threat actors and their methods to provide additional organization and controls to data or asset repositories.* *The Company maintains a threat or risk distribution list inside the organization, sharing as deeply as 'need to know' requires, and as widely as personnel awareness needs.*	***Process Specification Requirement*** P13-1 The Company gathers threat intelligence from multiple available sources to correlate with its current system configurations and risk posture. P13-2 The Company uses threat intelligence to develop new indicators of attack that can show new ways to recognize and react to threats. P13-3 The Company uses threat intelligence to update enterprise asset and system postures, informing both risk assessment and risk management processes. P13-4 The Company uses intelligence sources and recommendations for counteractions (e.g., ICS-CERT) to prioritize configuration changes and patch management efforts. P13-5 The Company uses internally-generated indicators and measures to correlate with external threat information. P13-6 The Company uses law enforcement or government security warnings to provide recognition training for espionage or insider threat indicators. P13-7 The Company uses threat intelligence on supply chain vulnerabilities to inform and shape vulnerability assessment, risk assessment, and vendor / third party vetting for contract goods and services that come into the enterprise.	***Information Technology Specification Requirements*** IT13-1 The Company utilizes internally developed or externally provided threat intelligence to attempt to characterize the methods, attack probabilities, potential impacts, and motivations of cyber threat actors against IT assets. IT13-2 The Company uses indicators of attack to review and renew security continuous monitoring log review rules, updating security information and event management (SIEM) rules as possible or as required. IT13-3 The Company uses threat intelligence to update data filter rules in intrusion prevention or intrusion detection systems, and in firewalls or heuristic detection systems. IT13-4 The Company uses periodic protective device intelligence feeds (i.e., for certain firewall systems) to update behavioral rules to screen system traffic. IT13-5 The Company uses web reputation systems to filter and block websites of less than a certain age, to reduce the potential impact of cyber-crime. IT13-6 The Company uses internally-generated threat intelligence for correlation with external threat intelligence indicators, including tripwires for (but not limited to): (1) Account lockouts; (2) Configuration modifications; (3) External activity to specific ports; (4) Login and access logs; (5) Former staff account activity; (6) Work hours and asset access mismatch; (7) Brute force logins; (8) Privileged account changes; (9) Remote mail logins from uncommon locations; (10) Systems accessed as administrator or root;	***Operational Technology Specification Requirements*** OT13-1 The Company utilizes internally developed or externally provided threat intelligence to attempt to characterize the methods, attack probabilities, potential impacts, and motivations of cyber threat actors against OT/ICS. OT13-2 The Company uses threat intelligence-based indicators of attack to review OT/ICS logs and log repositories, updating monitoring systems or devices as required to pace the threat. OT13-3 The Company uses threat intelligence on adversary methods to check safeguards and controls on interface systems, protocol converter systems, and monitoring systems that may have common components (such as web browsers) resident. OT13-4 The Company uses threat intelligence about potential threats and actors in the supply chain to inform vulnerability and risk assessment efforts for the OT/ICS.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		(11) Login traffic between test and production environments; and (12) User login from unusual numbers of simultaneous endpoints. IT13-7 The Company uses threat intelligence on actors and methods to help control and reduce attack surfaces within the enterprise, such as inventorying and controlling asset repositories.	
(14) Perform Vulnerability Assessment ***Best Practices Include*** *The Company runs periodic vulnerability scans against its systems, seeking gaps in protective coverage and in configuration of systems.* *The Company considers the connections of each system with reported vulnerabilities to determine the criticality of those vulnerabilities, and the priority to be assigned for patching those systems.* *The Company has a process by which recognized and discovered vulnerabilities from scans and asset assessments are fed back to the risk assessment process for prioritization and decisions on mitigation actions.*	***Process Specification Requirement*** P14-1 The Company employs an integrated process for vulnerability assessment that uses asset inventory and configuration information, matched against threat intelligence and vulnerability notifications, to inform current risk status, prioritize vulnerability remediation action, and update or modify boundary or perimeter controls and monitoring. P14-2 The Company keeps a prioritized list of assets with both vulnerabilities and exposures to potential threats to guide its patch management and internal testing and monitoring processes. P14-3 The Company uses vulnerability reports and threat intelligence to inform and shape systems procurements and acquisitions, the better to make secure systems a priority while avoiding systems or components known to present security vulnerabilities. P14-4 The Company uses vulnerability assessment of assets and operations to inform the risk management process of potential for insider threats to the enterprise. P14-5 The Company understands the time threshold for enterprise viability and operational impacts in case vulnerable systems are out of service as a result of a realized risk.	***Information Technology Specification Requirements*** IT14-1 The Company collects vulnerability notifications from appropriate, definitive sources (national CERTs, governmental agencies, CVE database) to determine hardware, software, and firmware or process vulnerabilities applicable to enterprise, system or platform assets. IT14-2 The Company conducts scans of its externally-visible Internet Protocol (IP) address space to determine exposures of its externally-facing systems to outside sources. IT14-3 The Company conducts vulnerability scans against interior network zones, inside the demilitarized zone (DMZ), to determine effectiveness of networked system segmentation and area segmentation. IT14-4 The Company uses vulnerability scans and tools to gauge effective compliance with system lockdown configurations (endpoint and server ports, protocols and services restrictions) and to correlate with perimeter protective device logs of ports, applications, IP addresses and user associated with the ports and applications. IT14-5 The Company uses administrative, managerial, operational or technical remediation or controls to address vulnerabilities found in its systems. Vulnerabilities of serious concern, but without ready mitigation available, may be addressed by removal of access to connectivity, i.e., removal of exposure to make the vulnerability much less possible to exploit.	***Operational Technology Specification Requirements*** OT14-1 The Company keeps, updates and maintains system interface descriptions and inventory to support risk and vulnerability assessment efforts. OT14-2 The Company reviews, evaluates, and communicates industry cybersecurity threats and OT/ICS strategies throughout relevant personnel in the enterprise. OT14-3 The Company runs periodic vulnerability scans on its OT interface systems and its OT/ICS to identify configuration discrepancies and gaps in protective coverage. OT14-4 The Company uses threat intelligence about potential threats and actors in the supply chain provide derive indicators of attack for OT/ICS vulnerability and risk assessment personnel. OT14-5 The Company considers vulnerability of network connections, transmission lines, and communications paths in assessment of relative weaknesses that could lead to system faults, service outages, or system failures, then provides this data for risk management and weakness mitigation. OT14-6 The Company performs vulnerability, impact, and criticality assessments before approving and/or prioritizing implementations of security patches that are intended to respond to reported vulnerabilities.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		IT14-6 The Company performs asset scanning for indicators of compromise (IoCs) and unexecuted malware on endpoints or servers. - Malware and indicators of attack (IoA) or indicators of compromise (IoC) - Unauthorized content - Unauthorized file transfers IT14-7 The Company conducts internal testing against its own assets to determine endpoint vulnerabilities (Operating System, mobile code, applications, firmware), network service vulnerabilities, infrastructure appliance or component vulnerabilities, and communication systems process vulnerabilities (i.e., potential for intercept in Last Mile). IT14-8 The Company conducts periodic reviews of its internal processes and procedures for potential gaps, looking especially at coverage percentages in vulnerability assessment; configuration assessment and query capability for endpoints; patch management coverage and timeliness of patch applications; and risk assessment summary reports to higher authority.	OT14-7 The Company conducts periodic reviews of its internal control system management, maintenance and operation processes and procedures for potential gaps, looking especially at frequency of system vulnerability assessment; configuration assessment and query capability for OT/ICS components; patch management capabilities, patch availability for individual systems and timeliness of patch applications; and risk assessment summary reports to higher authority. OT14-8 The Company uses monitoring technologies and/or processes to perform vulnerability scans.
(15) Perform Risk Management ***Best Practices Include*** *The Company uses a risk management method or conceptual framework to contain and contextualize all cybersecurity and related risk issues into a risk management and handling system.* *The Company does not pursue "perfected" security, but rather seeks a sustainable and acceptable risk posture that is economical, feasible, and supportable.* *The Company communicates information system and data risks in terms that its constituents will understand, relating to financial stability, brand reputation, and operations integrity.*	***Process Specification Requirement*** P15-1 The Company uses all available information from internal asset, process and operations sources, plus available information from external threat intelligence, vulnerability reports, and community lessons learned, to develop a comprehensive, enterprise-wide view of threats, vulnerabilities, and exposures to threat sources. P15-2 The Company uses a risk assessment and evaluation process that includes a review of vulnerabilities identified during internal asset scans and assessments when approving and prioritizing risk mitigation decisions.	***Information Technology Specification Requirements*** IT15-1 The Company uses a Risk Management Framework to consider and manage risks to the Company, its assets, data, systems and personnel. IT15-2 The Company uses risk assessment to determine Company-level risks in developing, fielding and operating new automated systems; each new system is subject to an independent risk assessment as part of portfolio risk management. IT15-3 The Company uses evidence-based security testing to inform its project risk management decisions, providing direction to software development and acquisition personnel in accordance with testing and relative risk of fielded applications or systems.	***Operational Technology Specification Requirements*** OT15-1 The Company uses a documented, systematic method or conceptual framework to guide cybersecurity and related risk decisions in OT/ICS systems. OT15-2 The Company's executive management proactively and periodically reviews organizational cybersecurity risks; the potential impacts of security breach events on enterprise functions, personnel, systems and environmental compliance; implemented protective practices; and related employee training.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company has defined a risk tolerance strategy, monitoring the risk indicators that support that risk tolerance strategy. *The Company leadership understands the regulatory and compliance environment that affects the Company and its operations, placing any factors which may change compliance reports in the risk register for risk management.* *The Company links security controls to the compliance reporting requirements, so that reporting indicates the degree of attainable security, not simple compliance.* *The Company defines risk to sufficient granularity as to allow intelligent use of risk sharing mechanisms, when the Company's cybersecurity maturity allows for the decisions that support sharing or transfer of risks.*	P15-3 The Company's executive management proactively reviews organizational cybersecurity risks, the potential impacts of security breach events, implemented protective practices, and related employee training. P15-4 The Company defines and details a process to periodically review existing IT and OT/ICS risks, identify and evaluate new risks, and update corporate tolerance for risks aboard marine or offshore assets. P15-5 The Company has a documented risk tolerance statement and risk management strategy that addresses technology and process areas across IT and OT/ICS within the enterprise context. P15-6 The Company seeks a risk posture based on factors (e.g., funding, feasibility, sustainability, etc.) defined and approved by corporate management. P15-7 The Company periodically reviews, tests, and assesses the effectiveness of the risk management plans at intervals not less than every two years**.** P15-8 The Company assesses IT Technical Debt and OT Technical Debt at the Risk Management Board on a periodic basis; Technical Debt is prioritized for accomplishment based on measured risk to the Company. Resource requirements to address Technical Debt shall be apportioned according to relative risk posed by each Technical Debt source, and forwarded for capital apportionment as required.	IT15-4 The Company uses its risk management information sources and aggregated view of relative risks to shape and direct the enterprise configuration and patch management processes, prioritizing system-level modifications through change management in order to implement software or system mitigation actions that head off the highest and most likely threats first. IT15-5 The Company uses its risk management information sources and aggregated view of relative risks as formative inputs to enterprise security architecture and engineering efforts. IT15-6 The *Company includes Business Continuity / Disaster Recovery systems, site(s) and facilities as part of the overall risk assessment and management effort.*	OT15-3 The Company classifies and prioritizes security risks (high to low) associated with each facility, afloat or offshore asset based on asset type (e.g., business partner association, age, capability, level of automation, associated certifying bodies, classification, etc.), including pertinent details for known security risks, change management procedures and procedure implementation, potential access points, established security zones, blocking devices, ICS network malware and intrusion protections, ICS communications channels to external networks, and any other communications conduits. OT15-4 The Company documents a failure consequence assessment (impact assessment) for each marine or offshore asset based on classified risks. OT15-5 The Company establishes corporate goals and measurement techniques (metrics) to be used as a basis for evaluating the effectiveness and execution of corporate ICS security program vis-à-vis potential risk conditions and effective management of those conditions. OT15-6 The Company determines and documents the impact and consequence(s) of a failure of each ICS function aboard each marine or offshore asset, referencing the asset-specific ICS-FDD and the ABS *ISQM Guide* for assignment of Integrity Level classifications to each major component. Determine and document the impact and consequence(s) of a failure of each ICS function aboard each marine or offshore asset. OT15-7 The Company establishes and documents a corporate baseline OT/ICS security risk and risk tolerance assessment for each marine or offshore asset based on the risk assessment methodology that identifies and prioritizes the impact and consequence(s) of a failure of each ICS function, considering security risks, vulnerabilities, and failure impacts for each marine or offshore asset.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
			OT15-8 The Company aggregates individual marine or offshore asset risk assessments into a baseline corporate risk assessment document, which states the combined corporate risk of OT/ICS security incidents, establishes the corporate tolerance for that risk, and states the corporate response to that risk as a charter for a corporate-wide ICS security program. OT15-9 The Company includes Business Continuity / Disaster Recovery systems, site(s) and facilities as part of the overall risk assessment and management effort, especially when considering human or environmental safety considerations.
(16) Provide Data Protection ***Best Practices Include*** *The Company identifies sensitive data assets that require protection to safeguard the business or mission.* *The Company classifies its critical data so that personnel understand what data must remain behind specific safeguards. Those data assets deemed too sensitive for unprotected systems or assets, especially mobile devices, must be included in the policies distributed to, and enforced through, all employees.* *The Company secures its communications paths through commercial providers' networks by encrypting their communications paths and data transmissions to and from critical systems and functions.* *All users' systems are backed up automatically to prevent accidental or inadvertent loss of data.* *The Company specifies use and control of its proprietary data in contracts with third parties who must have access to that data.*	***Process Specification Requirement*** P16-1 The Company builds and maintains awareness and inventory of data repositories and data stores throughout the enterprise, using this knowledge to size and manage perimeter protections, risk profiling efforts, and physical protections as required. P16-2 The Company organizes and classifies its data to confirm differing types and classifications of data remain protected to the appropriate level. P16-3 The Company requires that all enterprise data and assets be stored in Company-owned and approved data storage locations or drives. P16-4 The Company requires a risk assessment statement from any subordinate department that requires external storage for enterprise data. P16-5 The Company allows file storage in screened and vetted cloud services, disallowing all others. P16-6 The Company provides automated data backup capabilities for all workstations, both fixed and portable, in storage that is physically and logically separate from operational file systems.	***Information Technology Specification Requirements*** IT16-1 The Company provides logging capabilities on data access to sensitive data stores, asset types, or data locations. IT16-2 The Company provides secure data destruction methods for data disposal. IT16-3 The Company provides encryption on all data in motion (i.e., in transit) to external destinations by use of technical means such as public key infrastructure (PKI). IT16-4 When risk dictates, the Company requires all data in motion within the network to be encrypted (i.e., https everywhere). IT16-5 The Company requires all data at rest (i.e., in data shares or repositories) to be stored in encrypted states. IT16-6 The Company manages encryption keys separately from the data encrypted by those keys, and keys are never stored on the drives they encrypt. IT16-7 The Company uses perimeter protective systems to filter data being sent out of the Company, preventing data from being sent to unauthorized cloud services or destinations.	***Operational Technology Specification Requirements*** OT16-1 The Company backs up ICS computer systems based on a routine established and managed in compliance with corporate ICS Security Office policy. OT16-2 The Company backs up ICS software based on backup procedures established by corporate IT policy. OT16-3 The Company defines and rigorously controls or limits number and types of mechanisms that enable file input/output to and from operational technology networks.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company defines how it will exercise external providers' services (e.g., cloud services and applications) as part of expected operations. Any external service chosen must satisfy organizational requirements for data security and safeguarding. *The Company considers data and privacy protection to be equivalent to physical security in priority and consideration for asset protection.* *The Company actively protects the data paths between and among its various assets, sites or facilities, especially those geographically remote or in difficult-to-reach locations.*	P16-7 The Company understands the sensitivity and value of its data, and it places supervisory and strict control language in its contracts with third parties who may require access to enterprise data to fulfill contractual obligations for goods or services. P16-8 The Company integrates external computational resource (i.e., cloud) service providers with the overall data security and risk assessment processes to confirm data risk includes all storage and processing methods (source to sink) used in the enterprise. P16-9 The Company designates Privacy-related data, trains personnel on its handling procedures and methods, uses specific access clearances and authorizations to confirm accountability. P16-10 The Company establishes physical security procedures and measures to protect desktop computers and laptop computers from theft and unauthorized access where broader physical access control is not practical or possible. P16-11 The Company prohibits use of personal email servers or personal email for use with enterprise data. P16-12 The Company confirms that all systems or machines designated for disposal have all data storage (e.g., hard drives) removed and destroyed prior to equipment disposal.	IT16-8 The Company may specify particular types of data to be sufficiently sensitive that they will only be retained or used in terminal mode; the files may not be resident on any workstation, and they can only be accessed through virtual desktop (terminal) means. IT16-9 The Company checks backups for viability and effectiveness, testing backup data sets at random for both viability and hygiene (i.e., no malware) on a periodic basis. IT16-10 The Company confirms data backups are maintained offline and physically separate from main data repositories, preferably in a different physical location. IT16-11 The Company modifies machines intended for use with sensitive data to remove their ability to write data outside allowable methods; physical ports are blocked or removed, writable drives are removed, and local storage may add monitoring software to assist in audit of files retained on the endpoint. IT16-12 The Company uses physical locks or barriers to prevent storage medium theft from desktop machines (i.e., prevent storage drive theft).	
(17) Protect Operational Technology ***Best Practices Include*** *The Company integrates security requirements into operational technology safety cases, so that security testing will not invalidate or adversely affect safety tests, but while also including security as a fundamental part of system and human safety considerations.*	***Process Specification Requirement*** P17-1 The Company provides for senior leadership approval of, participation in, and support for ICS security programs, with a senior-level sponsor for ICS security activities. P17-2 The Company obtains senior management support for the ICS security program, including establishment of, and staffing for an ICS Security Office.	***Information Technology Specification Requirements*** IT17-1 The Company makes arrangement through the ICS Security Office and other organizational authorities as required for the physical security of infrastructure and interface gear that connects to OT/ICS.	***Operational Technology Specification Requirements*** OT17-1 The Company will conduct and document periodic and non-periodic ICS Security policy and procedure reviews upon the events including, but not limited to: • Changes to system architecture and hardware • Identification of evolving threat vectors • Changes to regulatory or class rules • Updates to customer requirements • Changes to information classification • Changes in public policy.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company restricts and filters all traffic from IT-based control systems to operational and process technology systems, so that authentication and verification of commands occurs outside the OT systems, software and appliances. *The Company uses signed copies of software updates to its systems, working only with manufacturers to obtain system updates and patches.* *The Company restricts access to ordinary Internet protocols and traffic (e.g., email, FTP, etc.) from machines authorized to connect to operational technology and process control systems.* *The Company uses 'optical data diodes' or similar functionalities for data transmission from critical components or systems to authenticated outside users in order to minimize potential for unauthorized outside access to those systems via data reporting mechanisms.* *The Company architects protective devices between information technology networks and operational technology networks to limit traffic types, protocols, and origins, and to trace and log all traffic into the operational technology network(s).* *The Company tracks and monitors the risk its production systems may present to neighboring organizations, and it communicates risks and incident management plans to those neighbors and/or community.* *The Company does not allow cyber-enabled systems that control, monitor, or record data from physical security systems to reside on the same control networks as the physical security systems.*	P17-3 The Company establishes and maintains an ICS Security Office to provide internal training for employee(s) and/or contractor(s); the Office has the authority and resources to develop, update, and communicate ICS Security policy. P17-4 The ICS Security Office confirms that lessons learned and threat intelligence are applied to the Company's OT/ICS to defeat attack methods used in attacks against others. P17-5 The ICS Security Office uses the Functional Description Document (FDD) as its primary tool to manage system operations, response and restoration, and the FDD is kept updated and complete. P17-6 The Company keeps other nearby organizations informed of risks and subsequent issues if OT/ICS may be affected, with potential impacts outside the asset or facility boundaries. P17-7 The Company uses fault tree analysis methods and failure mode analysis methods to find paths that can provide avenues of attack against critical systems. P17-8 The Company conducts failure mode analyses when considering system, process, or architectural changes in its operational and production systems. P17-9 The Company models and plans against cascading failures in its operational systems that could affect other systems, neighboring organizations, or the community. P17-10 The Company exercises due care and due diligence when assessing cybersecurity risks and implementing protective system processes and assets. P17-11 The Company resources physical and cybersecurity programs to sufficiently protect assets and information from expected security threats. P17-12 The Company specifically describes risk indicators that trigger effective and proactive risk prevention and resolution decision-making.	IT17-2 The Company limits the service functions available on control system interface systems or on protocol converter systems to the minimum necessary to satisfy control system (OT/ICS) interface functions; all general purpose functions (mail, file transfer protocol, telnet, etc.) will be disabled, and the limited ports, protocols and services (PPS) necessary for correct control system functions will be the only services open on these machines. IT17-3 The Company requires strict authentication on OT/ICS interface systems, requiring separate login from the general purpose network and two-factor authentication when administrative or control functions are to be exercised. IT17-4 The Company reduces its attack surface against OT/ICS from IT by (1) Isolating the ICS from any general purpose (untrusted) networks; (2) Locking down unused ports, and disabling remote access ports on servers and repositories; (3) Allowing external, real-time connection only required for mission or business purpose; (4) Designating single ports with tight restrictions for communications with ICS; and (5) Differentiating between needs for true real-time data and needs for summary reporting, to minimize ports left open for data streams. IT17-5 The Company does not allow cyber-enabled systems that control, monitor, or record data from physical security systems to reside on the same control networks as the physical security systems. IT17-6 The Company cross-trains cybersecurity personnel and operational technology engineers to keep communications between the enterprise engineering groups open.	OT17-2 The Company develops, documents and maintains ICS configuration and security hardening methods employed in the Company, and it requires protective or secured configurations from OT system suppliers to protect ICS equipment and services. OT17-3 The Company, through the ICS Security Office, establishes a cross-functional ICS Computer Emergency Response Team (CERT) to handle provisioning for Company-wide response for technical, operational, legal, and public outreach recovery from security incidents. OT17-4 The Company describes ICS security blocking and barrier device design for protecting the ICS from unauthorized access and non-essential communications; the plan includes schematics of the ICS with indications of access points and the barrier devices implemented for blocking the identified access points. OT17-5 The Company maintains a documented functional description of ICS and linked networked systems, including implemented protective systems with documented references to functional requirements (rather than the credentials or assurances of the protection provider/supplier). OT17-6 The Company performs periodic risk assessments, including reevaluations of enterprise assumptions and requirements for internal cybersecurity capabilities and system monitoring. OT17-7 The Company performs periodic reviews and updates for assuring currency of all software used to detect and protect the ICS from malware. OT17-8 The Company requires authentication of control system communication protocol traffic through its interface systems, providing traceability and accountability for all cyber-physical system actions.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company has manual backup capabilities for each critical operational function in the production flow, and it trains and exercises with the manual backup capabilities on a periodic basis. *The Company does not allow emergency backup capabilities, frequently associated with maintaining safety and safe shutdown capability, to be on the same communications networks or control systems as primary operational or mission systems.* *The Company cross-trains cybersecurity personnel and operational technology engineers to keep communications between the Company's engineering groups open.* *The Company uses fault tree analysis methods and failure mode analysis methods to find paths that can provide avenues of attack against critical systems.* *The Company conducts failure mode analyses when considering system, process, or architectural changes in its operational and production systems.* *The Company models and plans against cascading failures in its operational systems that could affect other systems, neighboring organizations, or the community.* *The Company defines and strictly limits the types and mechanisms for file input and output to and from operational technology networks.*		IT17-7 The Company defines and strictly limits the types and mechanisms for file input and output to and from operational technology networks.	OT17-9 The Company segments the OT/ICS network infrastructure away from the general purpose networks or business networks, using appropriate architectural and security protective devices to shield, conceal and protect systems from the untrusted networks, and to strictly control entry points for data into the control system networks. OT17-10 OT/ICS and reporting devices are connected to a protected network segment with limited, delineated access methods and protocols for both operators and other communicating machines. OT17-11 The Company confirms no administrative functions from general-purpose networks (mail, etc.) are available on OT or process control systems or interface systems, appliances or devices. OT17-12 The Company engineers wireless circuits and access points into control system areas, using best practices from network engineering (encrypted networks, certificates or complex passphrase access, logging of access and activity, strict accountability of access.) OT17-13 The Company manages public resources (e.g., wireless guest networks) by applying acceptable use policies or standards, user authentication techniques, and system address/port tracking methods OT17-14 The Company has manual backup capabilities for each critical operational function in the production flow, and it trains and exercises with the manual backup capabilities on a periodic basis. OT17-15 The Company does not allow emergency backup capabilities, frequently associated with maintaining safety and safe shutdown capability, to be on the same communications networks or control systems as primary operational or mission systems.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
			OT17-16 The Company requires that physical security equipment that is linked or linkable to computer networks remains operational and unaffected by power loss, software reboot, login failures, and/or system lockout. OT17-17 Define and assign roles and responsibilities required to support a baseline security risk assessment of each offshore or marine asset. Review participation in assessment team activities to understand that personnel/organizations having knowledge of the ICS implementation aboard each asset establish risk levels of tolerance. OT17-18 The Company vets, screens, authorizes, and credentials third-party personnel and systems prior to connection to proprietary networked systems. OT17-19 The Company describes and documents security actions, security supporting systems, and risk management processes in a unified cybersecurity architecture (e.g., reference model, framework, or logical construct). OT17-20 The Company verifies that protective system functions integrate with protective processes and assets to provide more complete operational security situational awareness. OT17-21 The Company develops, tests, and periodically trains staff on manual backup procedures for critical operational functions in the production flow.
(18) Perform System and Security Continuous Monitoring ***Best Practices Include*** *The Company monitors its security devices and their status reporting or dashboards, monitoring for proper function and for threats and risks revealed through log and alert reports.*	***Process Specification Requirement*** P18-1 Machine or system access to networked systems, data, personnel or enterprise functions is granted on the basis of least privilege, minimum required access, and continuous performance and security monitoring capabilities. P18-2 The Company implements a log review process, including lessons learned, additional recommendations for mitigation, and escalation to incident response.	***Information Technology Specification Requirements*** IT18-1 The Company performs database monitoring on database assets to confirm activities do not affect content or integrity negatively.	***Operational Technology Specification Requirements*** OT18-1 The Company develops and deploys an ICS security intrusion monitoring and alarming plan, design, and deployment, which includes a description of ICS security monitoring and alarming notification processes (including e-mail) for communicating and reacting to OT/ICS notices and alarms.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company monitors the entire network for security, not just the perimeter access points. *The Company uses outside activities for monitoring any systems that cannot be managed within the bounds of its existing capabilities and/or staffing strength.* *The Company performs security monitoring throughout the network, not just at the perimeter.* *The Company will monitor its guest wireless network to verify that resource is not used for illicit or unauthorized purposes, and to prevent malware from freely communicating through it.* *The Company will monitor its internal wireless networks to prevent unauthorized access points that grant access to the networked systems or infrastructure.* *The Company monitors performance and security of its own website(s) to maintain understanding of customer response and data security, and to prevent undetected fraudulent diversions of traffic and data.* *The Company identifies and uses a designated set of management or diagnostic tools for use in detecting and reporting anomalous or inappropriate behaviors.*	P18-3 The Company identifies the operations required to capture log records from networked systems, using operating system functions, network scripting, and network management applications to capture said log data; all systems that can generate logs and/or traceability output for user and system interactions shall provide logs in an organization-determined compatible output format. P18-4 The Company places priority for monitoring and anomaly detection on machine-to-machine communications, including service accounts. P18-5 The Company may review its own logs and security data, or it may contract a Managed Security Service Provider (MSSP) to perform those duties. P18-6 The Company requires all projects, programs, applications, systems and appliances that connect to the enterprise networks, systems or repositories to be reviewed, tested and approved by organizational security personnel prior to deployment and activation of such projects, systems, etc. on the enterprise network. P18-9 The Company strictly limits access to logs and log repositories to authorized personnel only. P18-10 The Company installs and monitors appropriate physical access control devices as designed and described in the Functional Description Document (FDD). P18-11 The Company monitors the physical environment at security access points and within secured physical boundaries described in the Company security plan and in the FDD to detect unauthorized access events that could lead to potential cybersecurity events.	IT18-2 The Company performs log management, apportioning storage as required to retain logs for sufficient time as to support defense against attack cycles; this may mean up to 12 months retention for some organizations. IT18-3 The Company confirms both Legal and Ethics & Compliance departments are aware of the parameters and data collected through the networked systems, and that they understand what data can be used to satisfy legal or compliance reporting. IT18-4 The Company accords priority storage and handling for logs and analysis supporting anti-insider monitoring. IT18-5 The Company designates logs and data streams from systems, applications and appliances that support behavioral monitoring and analysis as special interest for priority handling and storage allocation. IT18-5 The Company maintains logs and records associated with standard network access activities (login/logout). IT18-6 The Company maintains logs and records showing network resource access, especially repository or special asset access, or lateral movement across system domains or network segments. IT18-7 The Company monitors all network users' access methods when originating from outside the network periphery, including on virtual private network (VPN) access, and on network-specific, certificate-based access methods (e.g., Microsoft Direct Access). IT18-8 Any attempt to enumerate or query network servers, devices, appliances, applications, protective systems or infrastructure systems shall be alerted and reported immediately for controlling actions by organizational personnel.	OT18-2 The Company assigns a level of severity for each listed incident (e.g., Critical, Essential, Necessary, Low) that can be used to direct an appropriately scaled response to the incident. OT18-3 The Company maintains and actively monitors centralized host and network logging solutions after ensuring that all devices have logging enabled and their logs are being aggregated to those centralized solutions. OT18-4 The Company implements security data collection and control capabilities that inform both compliance reporting requirements, and analysis of the relative security attainable by the risk management program. OT18-5 The Company logs and reviews all remote login attempts, recording the time, date, duration, and source of all remote access events, and recording unsuccessful attempts (suspected probes) at remote access. OT18-6 The Company monitors OT/ICS and networked log analysis devices for indicators of attack including, but not limited to: (1) IP traffic on ICS boundaries for abnormal communications; (2) IP traffic within network for malicious connections; (3) Network hosts to detect malicious software and attacks; (4) User login time/place to detect stolen creds or improper access; and (5) User account or user administrative actions that are excursions from normal behavior. OT18-7 The Company develops and deploys an ICS security intrusion monitoring and alarming plan, design, and deployment, which includes a description of ICS security monitoring and alarming notification processes (including e-mail) for communicating and reacting to OT/ICS notices and alarms.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		IT18-9 The Company *monitors guest wireless networks to identify and prevent unauthorized activity, including the malicious or inadvertent introduction of malware.* IT18-10 The Company monitors all wireless networks to identify and disable or block unauthorized Network Access Points (NAP). IT18-11 The Company monitors and manages script execution instances (e.g., Microsoft PowerShell) with tools indicating actions performed on workstations or servers. IT18-12 The Company monitors activity meant to anonymize users, and enforces prohibitions against users employing such techniques as internal proxy servers, anonymizers, or The Onion Router (TOR) network access.	OT18-8 The Company maintains an updated inventory of security system devices, configurations, and settings for system maintenance, system evolution control, personnel training, and periodic protective system auditing. OT18-9 For automated alert responses systems, triggered alerts are captured, logged, managed by automated security response protocols, and reported for additional review/response to authorized personnel. OT18-10 The Company establishes nominal (baseline) system behavior and target metrics for ICS performance, and monitors that performance. OT18-11 The Company establishes and monitors performance variances for each ICS that indicate possible or actual security breach attempts, recording and reporting variances as indicators for needed analysis of anomalous ICS performance. OT18-12 The Company uses detected events to understand attack targets, penetration points, attack methods, and potential impacts on the ICS and connected systems; this information is then shared with vulnerability and risk management process owners. OT18-13 The Company performs the following upon detection of intrusion attempt against ICS: (1) Document and report all ICS security incidents by occurrence, severity, and type. (2) Document and report incident recovery measures and post-incident remediation impacts if any. (3) Log and review all access attempts. **(4)** To the extent practical, detected event data are aggregated and correlated from multiple sources and sensors in order to fully characterize the event.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
			(5) Provide all incident data to the Incident Response Team (IRT) for incident control, and to support lessons learned capture. (6) Document and report the description of impacts, (experienced and potential) with respect to safety, environment, production, lost-time, and cost (actual or anticipated if known). OT18-14 The Company uses monitoring technologies which, as deployed and documented in the Security FDD, are capable of detecting malicious code in the OT/ICS environment; unauthorized code or malware transmitted by mobile devices; or activities by remote or on-board external service provider(s). OT18-15 The Company uses monitoring technologies and/or processes deployed and documented in the Security FDD that are capable of detecting unauthorized personnel access to ICS equipment and computer controls, unauthorized electronic connections, the presence of unauthorized devices in proximity to ICS equipment, network and controls, and the presence of unauthorized software within the ICS.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
3- Protected Resources and Accesses			
(19) Plan for Disaster Recovery ***Best Practices Include*** *The Company defines the requirements and needs for business or mission continuity in face of threats and risk conditions, and plans against those risks so that the business can continue even through serious interference effects.* *The Company plans for, and resources, disaster recovery capabilities to provide continuity of business or mission capabilities when responding to risk conditions.* *The Company conducts periodic table-top exercises that allow revisit of disaster plans, initial training for new personnel, and refresher training for experienced personnel.* *The Company confirms that security architecture protecting the existing systems, facilities, personnel, and assets is adequately replicated in terms of functions during a disaster recovery scenario. Under no circumstance should a DR effort leave security undone.*	***Process Specification Requirement*** P19-1 The Company defines and documents business continuity requirements, identifies the threats to business continuance, and establishes plans for minimizing the risks and operational impacts associated with those threats, and documents the findings with the Risk Management process owner. P19-2 The Company documents its application and software portfolio to allow and encourage delineation of mission-critical, mission-essential and non-essential applications and systems in the enterprise. P19-3 Those applications in the mission-critical portfolio are included in recovery planning for organizational continuity. P19-4 Those applications in the mission-essential portfolio may be included in recovery planning for the Company, but on a case-by-case basis. P19-5 The Company, having defined cyber risk within the context of enterprise risk, uses risk sharing or risk transfer mechanisms against significant loss resulting from a cyber incident to defray costs during a business continuity or disaster recovery event. P19-6 The Company considers its relative position in its community and environment, determining as part of overall disaster recovery risk management whether organizational assets are critical to the functional continuity of the community, surrounding industrial entities, or regional/national infrastructure.	***Information Technology Specification Requirements*** IT19-1 The Company tracks all applications in the enterprise portfolio, maintaining a categorized list for those applications which must be included in recovery planning for organizational continuity. IT19-2 The Company organizes, maintains and periodically tests the facilities and systems which provide organizational continuity and disaster recovery capabilities. IT19-3 The Company applies the same data security and system security requirements and controls to the disaster recovery site and/or systems as to operational systems. IT19-4 The Company confirms its personnel and entities directories are available and replicated for use in maintaining operations and security throughout enterprise systems when operating the disaster recovery site and/or systems, or when operating under the organizational continuity plan. IT19-5 The Company conducts periodic “table-top” exercises to review and improve disaster plans.	***Operational Technology Specification Requirements*** OT19-1 The Company develops an OT/ICS availability and continuity plan that establishes business needs and quantifiable targets for availability and continuity. OT19-2 The Company develops business continuity plans, and is prepared to implement those plans in response to disasters and security incidents OT19-3 The Company builds and maintains an OT/ICS Recovery Action Plan for reestablishing normal safe operating conditions of the impacted personnel, systems, ship/ platform/ facility, including a plan for recovery from any detrimental environmental impacts. OT19-4 The Company confirms that the security architecture protecting personnel, systems, facilities and assets is functionally restored a part of the disaster recovery plans and procedures. OT19-5 The Company conducts periodic “table-top” exercises to review and improve disaster plans. OT19-6 The Company develops, tests, and periodically trains staff on manual backup procedures for critical operational functions in the production flow.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
(20) Provide Unified Identity Management ***Best Practices Include*** *The Company establishes and maintains consistent processes for managing identity and data access information about users, to establish who they are, to what groups they belong, how they are authenticated and what they can access among enterprise assets.* *The Company provisions and supports single sign-on (SSO) methods across systems, with governance decisions made concerning assets that must require specific, separate login for access traceability.* *The Company establishes identity governance processes involving all organizational stakeholders (application owners, human resources department, payroll department, IT department, and data owners) to provide accurate, timely, and auditable operational processes for user provisioning and de-provisioning.* *The Company uses measures and metrics to gauge effectiveness and improvements in the various identity processes that span departments or divisions, including such areas as times to provision or de-provision access; frequency of directory cleanup sweeps; numbers of shared or group credentials; numbers of failed logins, and lockout frequency; etc. This data is useful for process improvement, and it also serves as very useful input to log examination and management.* *System and data access are apportioned on the basis of user roles, job responsibilities, and role attributes, which data is maintained in the master human resources data repositories for authoritative sources.*	***Process Specification Requirement*** P20-1 The Company defines and documents role-based identity requirements that tie employee identity across enterprise assets and privilege grants. P20-2 The Company establishes and deploys processes linking Human Resources (job requirements and qualifications) to IT (system and asset access and privilege levels) for unified identity management across systems and processes. P20-3 The Company's identity management system provides rigorous, accurate, timely, and auditable user identification and user access provisioning and de-provisioning processes that are consistent across the entire enterprise. P20-4 The Company gauges and periodically evaluates the effectiveness of its identity management system and processes by evaluating system metrics (e.g., provisioning activities, shared credentials, failed logins and lockout frequency). P20-5 The Company grants administrative privileges to only those personnel in roles requiring the capability to make changes to machine configurations, and to no others. P20-6 The Company requires that system administrators will only use administrator roles and privileged credentials for maintenance and system administration or management duties; for all other duties, administrators shall use normal, restricted-privilege user accounts.	***Information Technology Specification Requirements*** IT20-1 The Company *establishes and maintains identity management processes (1) for identifying controlled asset users and user groups, (2) for enrollment of authorized users of controlled enterprise assets, (3) for authenticating controlled asset access privileges, and (4) for initialization and removal of user access privileges and credentials.* IT20-2 The Company provides user access privileges depending on and in proportion to stated job attributes, roles, and responsibilities as documented and maintained in an authorized HR database. IT20-3 The Company promptly and proactively deactivates authorization credentials and accounts of employees and third parties who no longer require access to proprietary systems. IT20-4 The Company promptly and proactively deactivates authorization credentials and accounts of employees who are voluntarily or involuntarily terminated. IT20-5 The Company restricts and filters traffic from IT based controls systems so that authentication and verification commands occur outside of Operational Technology systems, software and appliances. IT20-6 The Company implements login failure methods that time-out unused network connections and detect and prevent password guessing activities. IT20-7 The Company provides or limits single sign-on (SSO) credentials and services based on specific work-related needs and security criteria identified in its cybersecurity framework or architecture. IT20-8 The Company prohibits group login and/or shared credentials.	***Operational Technology Specification Requirements*** OT20-1 The ICS Security Office defines roles and responsibilities for operating, monitoring, and maintaining deployed detection technologies and processes, and documents in job descriptions to confirm accountability. OT20-2 The Company defines and implements role-based business rules for logical access to any Company ICS. Authorization of access is based on job function requirements and risk assessment processes. OT20-3 The Company maintains a record of all role-based accounts for each ICS aboard each marine or offshore asset and a record of all users assigned to each role-based account, especially for all administration level (privileged) access. Remove any user from the record that no longer requires access to a role-based account. OT20-4 The Company uses a defined and detailed process for permitting and controlling access to role-based accounts for all Company ICSs. OT20-5 The Company identifies the local authority responsible for approving or denying access to any role-based account on Company ICSs. OT20-6 The Company logs and reviews all access attempts, deactivating or suspending accounts that are not required for normal operation and maintenance activities (e.g., Supplier-activated accounts, Shipyard and super-user accounts, etc.). OT20-7 The Company defines the frequency and/or events that trigger password changes to all role-based accounts (e.g. new well site, crew change, security breach, post vendor upgrades, etc.).

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		IT20-9 The Company requires two-factor authentication for local and remote access to sensitive resources or assets. IT20-10 The Company prohibits and blocks Internet access for systems having privileged access account credentials. IT20-11 The Company uses a privileged account password escrow process to confirm that administrator account credentials cannot be stored on any machine, and to provide transparency and traceability of administrator actions.	OT20-8 The Company protects against unauthorized logical access to proprietary operational and protective systems using segregated communications paths, screening mechanisms, access control processes, identity system enrollment and role designation, strong passwords, and/or multifactor authentication. OT20-9 The Company requires that physical security equipment that is linked or linkable to computer networks (e.g., sensors, cameras, locks, network access points) is protected where possible from unauthorized access by means of strong, non-default passwords. OT20-10 The Company prohibits sharing of authentication resources or credentials between IT and OT/ICS.
(21) Perform System Software and Application Testing ***Best Practices Include*** *The Company has an authorization process for software upgrades that does not allow unexpected, unattended, or unauthorized software to be loaded in critical systems, or in operational systems that connect to critical systems.* *The Company tests all software for functional and security requirements prior to making that software available to users. Any software found lacking in the test process is not installed.* *The Company uses a periodic security evaluation tool and process to assess its current status, any gaps in security coverage, and outstanding requirements that may affect its overall security profile.* *The Company has internal audit capabilities for cybersecurity, and those personnel understand the cybersecurity context of the Company.*	***Process Specification Requirement*** P21-1 The Company uses test procedures and processes on any software, firmware or hardware installation, replacement, upgrade, or modification to existing functional portfolios, systems or components prior to the new or upgraded materiel being applied to the ship, platform or asset. P21-2 The Company tests system patches and software updates prior to their application to production systems; unclear or unsatisfactory test results must lead to refusal to load the software. P21-3 The Company tests system and application patches on a simulation or emulation test bed prior to applying the updates or patches to operational systems. P21-4 The Company implements security procedures for system development and software maintenance changes, with security tested throughout development.	***Information Technology Specification Requirements*** IT21-1 The Company uses test to build knowledge of any new hardware, software or firmware proposed for use in the enterprise, and the test process will replicate the operational environment to the best possible extent. IT21-2 The Company uses a testbed to provide a separate and safe environment to conduct software testing without the possibility of affecting the operational (production) system(s). IT21-3 The Company develops a method set and a toolkit for use in (1) functional testing and (2) security and safety testing. IT21-4 The Company uses standard test procedures to test software proposed by enterprise personnel to gain authorization to load on enterprise systems. IT21-5 The Company tests vulnerability remediation actions, mitigations, configuration changes and patches, and said modifications are approved by change management authorities after completion of satisfactory testing, and prior to installation.	***Operational Technology Specification Requirements*** OT21-1 The Company uses test to verify that default access methods, passwords or system access roles on operational systems have been changed after installation and configuration. OT21-2 The Company requires that any devices, systems, appliances or applications authorized and approved for remote access meet organizational policies for security, including pre-use testing in all allowed operating modes. OT21-3 The Company performs patch viability and system vulnerability testing prior to approving and/or prioritizing implementations of security patches that are intended to respond to reported vulnerabilities. OT21-4 The Company conducts ongoing test series to verify correct operation of installed systems in the enterprise, including (but not limited to)

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P21-5 The Company tests all software for functional and security requirements prior to approving the installation of software made available to users, and denies installation privileges to software that does not meet test requirements. P21-6 The Company provides testing personnel a training regime to match the expected standards for functional and security training, and training for the tools to perform the testing to standards. P21-7 The Company emphasizes integration, interoperability and functional inheritance (I3) in all testing, seeking areas of incompatibility or functional faults that may introduce risk conditions to systems or to other applications. P21-8 The Company does not allow software or systems to be loaded into operational endpoints, servers, devices or systems without successful, completed tests leading to change control authorizations.	IT21-6 The Company tests all software for functional and security requirements prior to approving the installation of software made available to users, and denies installation privileges to software that does not meet test requirements.	1- Security system detection technologies and processes are tested on a routine basis in accordance with a test plan documented in the Security FDD. 2- Intrusion detection technologies and processes are routinely assessed for performance and updated as needed to confirm that capabilities are current and continuously improved. 3- ICS security incident detection processes and technologies performance is regularly assessed. OT21-5 The Company conducts on-asset, no-notice, non-periodic OT/ICS security evaluations based upon security breach incidents, reported or discovered non-conformance to required documentation, or repeated gap findings during annual audit cycles.
(22) Perform System and Application Patch and Configuration Management ***Best Practices Include*** *The Company catalogs its hardware configurations and software holdings and licenses so that it can prioritize and apply patches that address identified vulnerabilities arising from threat reports, vulnerability scans, or risk analyses.* *The Company tests system and application patches on a testbed prior to applying the patches to operational systems.* *The Company understands and controls the use of applications and executable software in its systems, and it restricts any software from running unless the software has been tested and approved for use (whitelisting).*	***Process Specification Requirement*** P22-1 The Company has an active configuration management program that address all servers, endpoints, infrastructure components, and safety-critical or mission-critical systems, devices, applications and appliances. P22-2 The Company's technology leadership and governance authorities consider the configuration management and patch management strategies, logs of unmitigated vulnerabilities, and records of obsolescent or deprecated systems and software, to address coverage for all networked assets, relative risk within the networks, and updates to risk postures for the Company.	***Information Technology Specification Requirements*** IT22-1 The Company performs configuration management of all servers, endpoints, infrastructure components, network applications and utilities, and safety-critical or mission-critical systems, devices, applications and appliances. IT22-2 The Company uses community reporting, threat intelligence, manufacturer or software publisher reports, and any other sources to identify at-risk candidates for patching. IT22-3 The Company's standard configuration for provisioned systems is maintained in accordance with cyber hygiene best practices, and only changed through Change Management Process.	***Operational Technology Specification Requirements*** OT22-1 The Company performs configuration management on all OT/ICS interface devices, protocol converters, ICS components, ICS software, cyber-physical actuators and systems, sensors and data capture or aggregation gear, and special attention is paid to safety-critical or mission-critical systems, devices, applications and appliances. OT22-2 The Company maintains a log or records of OT/ICS systems or components that cannot be patched due to obsolescence, loss of manufacturer support, or inability to shut systems down, and this log forms an input source to the Risk Management Process.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P22-3 The Company uses configuration management for operating system and application software patch tracking and implementation; machine configurations for lifecycle management; and application version control across the Company. P22-4 The Company uses vulnerability assessment data to assign priorities to configuration management actions, with specific attention to systems designated as high-risk, safety-critical or mission-critical. P22-5 The Company uses security systems (perimeter protective systems, heuristic systems, endpoint scanners, etc.) to inform and update configuration management personnel on potential issues that have violated whitelisting and/or have changed server, appliance, application, and endpoint or device configurations. P22-6 The Company uses configuration management of security systems (perimeter protective systems, heuristic systems, endpoint scanners, etc.) to assist in managing ports, protocols and services allowed and used across the enterprise. P22-7 The Company maintains a software configuration management systems that registers all enterprise software assets and licensed code, including firmware in mission-critical or safety-critical systems. P22-8 The Company maintains a hardware configuration management system that registers all enterprise assets within the systems under management. P22-9 The Company tracks software versions, both installed and stored (inactive or not used), that are relevant to operations, operational systems and organizational capabilities, as part of the Functional Description Document.	IT22-4 The Company performs active patching and patch management on all assets, addressing vulnerabilities, obsolescence, renewed code, functional updates, or incompatibilities. IT22-5 The Company tracks reports of vulnerabilities or attacks against assets similar to what it holds and uses, and also tracks aging of vulnerabilities or reported obsolescence to maintain a complete picture of what must be patched, what is advisable or can be patched, and what has been patched. IT22-6 The Company confirms that patches assigned for deployment and application to endpoints, servers or infrastructure are tested and approved for application by Change Management prior to deployment. IT22-7 The Company keeps a log or record of patches, updates, upgrades or replacements with the appropriate systems, devices, appliances or application software records, matching the approvals of Change Management. IT22-8 The Company only receives and uses patches from known and trusted sources, giving priority to authenticated vendor websites and signed software updates or patches, to minimize the possible contamination of the patches with malware or unwanted programs. IT22-9 The Company uses out-of-band communications to communicate with the manufacturer or publisher of software in mission-critical or safety-critical systems, to minimize the potential for system compromise if network intrusion is suspected. IT22-10 The Company validates patches and software upgrades with authentication information from the manufacturer or publisher prior to loading the software components on any organizational machines, including test systems.	OT22-3 The Company maintains an inventory of critical components that must receive special attention when being patched or modified, including data encryption systems or applications, and safety-critical systems. OT22-4 The Company maintains a version-specific inventory of all OT/ICS software for each system, with master copies kept in safe storage and backup copies retained off-site. OT22-5 The Company references the ICS-FDD software inventory for ICS evolution control, system maintenance, personnel training, supplier management, and periodic ICS internal and regulatory audits. OT22-6 The Company uses project management and change management processes to update the ICS-FDD, its related documentation and all diagrams, as projects complete, systems are integrated, and applications are loaded into the network. OT22-7 The Company integrates cybersecurity and process safety management (PSM) change management procedures to confirm security is included with safety-critical system modifications. OT22-8 The Company uses threat intelligence about potential threats and actors in the supply chain provide derive indicators of attack for OT/ICS vulnerability and risk assessment personnel. OT22-9 The Company runs periodic vulnerability scans on its IT-based OT interface systems and its OT/ICS to identify configuration discrepancies and gaps in protective coverage. OT22-10 The Company performs vulnerability, operational impact, and criticality assessments before approving and/or prioritizing implementations of security patches that are intended to respond to reported vulnerabilities.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P22-10 The Company uses the FDD to track software inventory and software and firmware versions or requirements for each OT/ICS asset, using hardware vs software version limitations as an input to Change Management and budgetary processes. P22-11 The Company manages software updates and patching of installed software, including firmware, to confirm awareness of the update or patch; satisfactory testing of the update or patch prior to installation; approval by relevant organizational authorities of the update or patch prior to application or installation; special attention to updates or patches applied to either mission-critical or safety-critical systems prior to installation; and post-installation system testing to confirm full functional capacity in the updated or patched system. P22-12 The Company tests system and application patches on a simulation or emulation test bed prior to applying the updates or patches to operational systems. P22-13 The Company maintains a list of authorized software update and/or patch sources and only accepts software updates from those recorded sources for systems installed in the system, ship, asset or facility. P22-14 The Company takes steps to prevent inadvertent or unexpected software insertion or updates by such actions as: 1- Removal of user administrative privileges on individual systems; 2- Disabling or removing access to optical drives; or 3- Disabling or removing access to USB drives.	IT22-11 The Company maintains known software configurations that have been tested, proven and documented; these configurations form the baseline for patch testing and, after successful testing, patch application. IT22-12 The Company limits connectivity to trusted systems to confirm inadvertent connections or exchanges with untrusted networks or systems are minimized. IT22-13 The Company requires vetting of third parties who bring software or firmware updates, patches or upgrades from vendors, integrators or manufacturers, to include (at least) malware scanning of media and software; portable device scans for cyber hygiene prior to connection of any device to the organization network; and identity verification of these personnel prior to allowing them contact with critical systems. IT22-14 The Company requires that any remote patching performed by manufacturers, software houses or integrators be performed with organizational personnel managing the remote connections, monitoring the equipment or applications, and terminating the remote connections when completed. IT22-15 The Company performs monthly active scans of the network and all segments for new assets, sensors and/or machines, combining tools and results with vulnerability assessment scan activities.	OT22-11 The Company considers vulnerability of network connections, transmission lines, and communications paths in assessment of relative weaknesses that could lead to system faults, service outages, or system failures, then provides this data for risk management and weakness mitigation. OT22-12 The Company approves and documents ICS software changes and patches using a Management of Change Request (MoCR). Complete the MoCR according to instructions that describes the proposed patch and provides installation, test, and rollback instructions as required by the MoCR support documentation. Approve all MoCR submissions according to instructions included in the MoCR information materials prior to installation of any ICS software patch, change, update, or revision. OT22-13 For applicable ICS functional component systems, the Company requires use of an authorized, dedicated ICS Laptop with Change Management software to deploy approved changes to any PLC's and SBC's as needed. Confirm that all applicable hardware is on hand to integrate with the system. OT22-14 The Company requires approved software modifications to be conducted under secure conditions, with organizationally-specified security procedures, resources and facilities used to remove as much potential risk or uncertainty from the modification operations as can be expected. OT22-15 The Company requires any systems with remaining or outstanding, uncompleted patches, to be included in the ICS Technical Debt log for tracking through the Risk Management process. OT22-16 The Company will use architectural and access-based controls for legacy systems or for devices (i.e., Industrial Internet of Things) that are unpatchable or unsecurable in working configurations.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
(23) Execute Change Control ***Best Practices Include*** *The Company has an authorization process for hardware, software, firmware, and architecture or configuration upgrades that does not allow unexpected, unattended, or unauthorized changes to be made to critical systems, or in operational systems that connect to critical systems.* *A formal, rigorous change control process is critical to documenting both information technology and operational technology systems, maintaining enterprise knowledge of both, and implementing cybersecurity controls and security.* *The Company maintains logs, system diagrams, and records for all business-critical or mission-critical systems that note the changes made during the change control processes.*	***Process Specification Requirement*** P23-1 The Company maintains and uses a change management and control process that requires governance decision making prior to system updates or changes that could affect system, server, endpoint, device, appliance or software application performance, security status, or data reporting. P23-2 Change control is a requirement prior to configuration changes in hardware, software or firmware, requiring concurrence from accountable and responsible officials in the Company in order to proceed with installations, updates or patches. P23-3 The Company integrates cybersecurity and process safety management (PSM) change management procedures. P23-4 The Company reviews, updates, and maintains IT and ICS change management policies and procedures; periodic reviews of IT and ICS operations and change management policies and procedures help the Company maintain currency and confirm that IT and ICS security changes do not increase risks to safety or business continuity. P23-5 The Company approves all vulnerability remediation actions, mitigations, configuration changes and patches by change management authorities after completion of satisfactory testing, and prior to installation. P23-6 The Company conducts failure mode analyses when considering system, process, or architectural changes in its operational and production systems.	***Information Technology Specification Requirements*** IT23-1 The Company uses change control to make risk decisions about hardware, firmware and software updates with regard to operational software and potential impacts of changes on the enterprise. IT23-2 The Company uses change management to track and update the enterprise systems architecture, registering changes to documentation of systems and functions that make up the enterprise system of systems. IT23-3 The Company maintains records, logs, and system diagrams describing changes made to all business- or mission-critical systems and formalized in the change control system. IT23-4 The Company uses asset management databases and asset enumeration or query tools to confirm that a complete and accurate automated system inventory is maintained to support configuration and change control processes and procedures. IT23-5 The Company requires maintenance and repair of assets to be approved prior to start; recorded for change management of systems and configurations; and performed and logged in a timely manner, with controlled tools. IT23-6 The Company confirms subcontractor change management practices in compliance organizational or Company software management of change (SMOC) policy and procedures. IT23-7 The Company maintains an updated inventory of security system devices, configurations, and settings for system maintenance, system evolution control, personnel training, and periodic protective system auditing.	***Operational Technology Specification Requirements*** OT23-1 The Company understands and asserts that a rigorous, formally documented change control process is critical to maintaining engineering control over the evolution of information and operational technology systems. OT23-2 The Company maintains records, logs, and system diagrams describing changes made to all business- or mission-critical systems and formalized in the change control system. OT23-3 The Company maintains strict control over additions, deletions, and changes to software supporting critical systems, and to software supporting systems that connect to critical systems. OT23-4 The Company uses asset management databases and asset enumeration or query tools to confirm that a complete and accurate automated system inventory is maintained to support configuration and change control processes and procedures. OT23-5 The Company requires maintenance and repair of assets to be approved prior to start; recorded for change management of systems and configurations; and performed and logged in a timely manner, with controlled tools. OT23-6 The Company confirms subcontractor change management practices in compliance organizational or Company software management of change (SMOC) policy and procedures.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		IT23-8 The Company tests all software for functional and security requirements prior to approving the installation of software made available to users, and denies installation privileges to software that does not meet test requirements. IT23-9 The Company tracks and manages obsolete equipment and software assets to reduce or eliminate vulnerabilities presented by unauthorized access to and the use of those assets.	OT23-7 Approve and document ICS software changes and patches using a Management of Change Request (MoCR). Complete the MoCR according to instructions that describes the proposed patch and provides installation, test, and rollback instructions as required by the MoCR support documentation. Approve all MoCR submissions according to instructions included in the MoCR information materials prior to installation of any ICS software patch, change, update, or revision. OT23-8 The Company implements OT/ICS change management procedures aboard each offshore or marine asset, including all software change proposed by suppliers, using the Management of Change Request (MoCR). OT23-9 The Company, in order to protect against inadvertent or malicious introduction of malware into the ICS during shipment from the supplier, installation aboard vessels, and changes made during final acceptance test procedures and sea trials, uses change management procedures provided in the "ICS Management of Change Processes" section of this policy including the Company's Management of Change Request (MoCR). OT23-10 The Company maintains an updated inventory of security system devices, configurations, and settings for system maintenance, system evolution control, personnel training, and periodic protective system auditing. OT23-11 The Company will back up OT/ICS computer systems based on a routine established and managed in compliance with corporate IT policy. OT23-12 The Company stores accessible backup copies of ICS software available aboard each ICS equipped asset, and storing additional accessible backup copies of ICS software on shore for rapid delivery to marine or offshore assets as needed.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
			OT23-13 The Company tests all software for functional and security requirements prior to approving the installation of software made available to users, and denies installation privileges to software that does not meet test requirements. OT23-14 The Company makes a formal determination of ICS system and software to be decommissioned, logging the details of the ICS system decommission in the software registry (e.g., removed/destroyed; removed/archived; not removed / disabled; etc.), then retiring licenses through IT or OT management services for accounting purposes. OT23-15 The Company documents the architectural and functional impacts of the retirement of specific ICS in ICS-FDD. OT23-16 The Company tracks and manages obsolete equipment and software assets to reduce or eliminate vulnerabilities presented by unauthorized access to and the use of those assets.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
CS3: Integrated Capability Specification			
1- Practices, Programs, and Processes			
(24) Execute Capital Planning and Investment Control ***Best Practices Include:*** *The Company performs capital programming for networked systems and assets as a decision-making process to integrate strategic planning budgeting, procurement and technology management all in support of the Company's mission and business processes.* *The Company prioritizes key risk areas for investment and improvement to keep risks understood and manageable. The prioritized areas are consistent with the publicized budget goals and objectives.* *The Company uses capital planning and investment control processes to align enterprise technology with the Company's overall enterprise architecture and enterprise objectives.* *The Company considers security as at least equivalent to economics when pursuing system, process, or architecture changes.*	***Process Specification Requirement*** P24-1 The Company uses the periodic budget process to review and update functional controls and protective features in the systems security architecture. P24-2 The Company tracks and manages security technical debt (i.e., unmet security requirements) and considers the list of pending needs in relation to the Company's relative risk position. P24-3 The Company uses vulnerability reports and threat intelligence to inform and shape systems procurements and acquisitions, considering known vulnerabilities in systems or components under consideration to help determine future labor and resource requirements in security implementations. P24-4 The Company considers the economic and security tradeoffs of maintaining a heterogeneous architecture that could make successful intrusions more difficult. P24-5 The Company includes Business Continuity / Disaster Recovery capabilities as part of the enterprise capability requirements for appropriate funding and executive attention. P24-6 The Company monitors trouble reports, test results and help desk tickets on software and the enterprise software portfolio to understand the enterprise risk posture, using compiled results for governance decisions regarding allocation of investment to reduce security or functional risks in the enterprise.	***Information Technology Specification Requirements*** IT24-1 The Company confirms IT technology refresh and system lifecycle management costs are integrated in budget management processes. IT24-2 The Company includes security architecture costs and risk management expectations in the balance for capital expenditures. IT24-3 The Company procures components and assets for networked systems that have consistent vendor support, administrative manageability, and which implement industry standards for security. IT24-4 The Company monitors system program performance in the overall systems architecture to manage progress of cost, schedule and performance against expected organizational mission benefits. IT24-5 The Company tracks cryptographic and data protection requirements in terms of threats to data and enterprise-standard hardware, and it confirms capital budgets reflect periodic needs for computational upgrades to support increasing cryptographic protections. IT24-6 The Company tracks all software projects, applications, systems or components which have security test and evaluation (ST&E) discrepancies as a result of inherited enterprise issues, i.e., downstream or host system present vulnerabilities that affect the software under test, as IT Technical Debt to be addressed in governance and capital planning.	***Operational Technology Specification Requirements*** OT24-1 The Company confirms OT/ICS technology refresh and system lifecycle management costs are integrated in budget management processes. OT24-2 The Company includes security upgrades and system monitoring requirements in the budget process for capital improvements to OT/ICS. OT24-3 The Company plans and budgets for retirement, decommissioning, and/or disposal of OT/ICS components and systems in the capital planning process. OT24-4 The Company tracks all OT/ICS software components which have security test and evaluation (ST&E) discrepancies as a result of inherited enterprise issues, i.e., downstream or host system present vulnerabilities that affect the OT/ICS, as OT Technical Debt to be addressed in governance and capital planning.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
(25) Implement Architecture Management ***Best Practices Include*** *The Company's security projects are under specific, accountable control for effective accomplishment and deterministic contribution to the Company's systems architecture.* *The Company uses architectural and design features to limit possible intrusions and illicit movements within the Company's networked boundaries, giving additional time for detection and defeat of unauthorized access.* *The Company considers traffic patterns and flow in architectural and design choices of transmission systems and protocols, and it plans for traffic capacity in choices of operational technology nodes and components.* *The Company does not allow cyber-enabled systems that add capabilities to physical security systems to reside on the same control networks as the physical security systems.* *The Company will not allow equipment emplaced for maintenance, prototyping, experimentation or proof-of-concept development to remain in place after the conclusion of the operation, especially if that equipment included communications connections or interfaces that were not documented as part of the main systems' architectures.*	***Process Specification Requirement*** P25-1 The Company implements separate management methods and means for IT and OT systems and networks. P25-2 The Company uses Enterprise Architecture to bring a common structure and interoperability to systems and projects that are integrated into the overall networked infrastructure. P25-3 The Company uses the standards and policies governing the Enterprise Architecture and the security architecture to levy data interoperability requirements on integrating systems, specifically requiring instrumented, sensor or system data feeds into the centralized security monitoring systems architecture in order to build system visibility into the networks. P25-4 The Company architects cloud service - system connections to be monitored for data exfiltration, with appropriate involvement from business users of the cloud services. P24-5 The Company considers the economic and security tradeoffs of maintaining a heterogeneous architecture that could make successful intrusions more difficult. P25-6 The Company requires auditable functional similarity in security programs and policies between reporting units, enterprise systems, and subsidiaries within the enterprise, and it implements policies and plans to bring about security and operational similarity. P25-7 The Company requires applications to implement encryption protocols on all internal and external communications paths between and among components, modules and data repositories. P25-8 The Company confirms that public-facing web systems place databases on separate assets, away from the web server and web application(s). Databases serving web applications are appropriately located behind the DMZ firewall within the security architecture.	Information Technology Specification Requirements IT25-1 All IT systems are present on system diagrams kept up to date with changes to systems, data flows, major sensor systems, and functional system connections to OT to maintain visibility over the networked system of systems on the asset or in the facility. IT25-2 The Company requires every system, appliance, application, server or repository on the production network to be governed by organizational rules for change control, change management and configuration management. IT25-3 The Company's architecture requires and provides authoritative sources for Network Time Protocol (NTP), and all network servers, communications systems (e.g., VPN), and applicable appliances point to the authoritative source for central time coordination. IT25-4 The Company requires organizational data to be labelled, classified or categorized by either manual or automated means prior to storage in repositories in order that the data may be controlled for access by use of the labels. IT25-5 The Company requires systems and projects which deliver hardware to the production networks, either wired or wireless, to provide: 1. Architectural diagrams and system construction details for Security to understand the system prior to its full development; 2. Expected (inherited) services, ports, protocols or services; 3. Identifying information about devices, servers, systems, etc. that allow Security to gain visibility of the system as it goes into test. Media Access Control (MAC) identifiers, communications protocols, and any other data required for understanding and integration of the system(s) into the architecture.	***Operational Technology Specification Requirements*** OT25-1 All OT systems are recorded on system diagrams kept up to date with changes to systems, data flows, major sensor systems, and functional system connections to IT to maintain visibility over the networked system of systems on the asset or in the facility, and to keep incident response procedures updated and effective. OT25-2 The Company creates segmented networks to contain OT/ICS, with asset separation and distinct credentials for access to each segment or system. OT25-3 The Company segregates networks supporting emergency backup processes and systems that are frequently associated with safety and shutdown capabilities from operational or mission critical system networks. OT25-4 The Company builds a defensible environment for OT/ICS by segmenting ICS away from IT, restricting host-to-host communication paths outside the segmented enclave(s), and consolidating all potentially vulnerable OT/ICS devices and systems within the protected, safe zone. OT25-5 The Company's OT/ICS architecture and system restrictions on ICS enclaves force any inserted media or entering data through scanning, screening and filtering to confirm communications are authorized, of the proper protocols and formats, and contain no unauthorized code. OT25-6 The Company will, where possible, engineer, install and configure OT/ICS in ways that assist in data flows and component management through technical monitoring means.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P25-9 The Company exercises architectural governance over networked resources by periodic review of network structures and architecture as built, taking opportunities to rationalize and consolidate networks in order to confirm consistent and universal security is maintained throughout the enterprise. P25-10 The Company consciously minimizes the number of external connections to Internet or communications systems to confirm that all external communications paths, on either IT or OT systems, are properly screened and monitored.	IT25-6 The Company requires initial security requirements of all systems or projects which deliver hardware or software to the production networks, either wired or wireless, to include: 1. All systems - internal and external – and projects that communicate with hypertext protocols shall use secure http methods and ports. Unprotected http over port 80, which allows cleartext (unencrypted) transmissions of usernames, passwords, other login information, and application information, is specifically forbidden on the enterprise networks. 2. All systems shall use enterprise certificates for authentication within the networked environment. 3. All systems shall be reconfigured for default password changes in all components and systems that contact the production network, or which contact systems on the production network. No systems not specifically meant to have access to the Internet shall be allowed to have access to the Internet. 4. Web-based systems shall refer all user authentication to enterprise systems for both authentication and authorization permissions. 5. No user credentials, including credential hashes, shall be retained on any web server or web database, or by any web application. 6. Web applications may be authorized to conduct their own user authorization and accounting after a successful authentication, assuming their access management methods can be demonstrated to be secure. IT25-7 The Company architects software applications, systems and components for storage and processing resources appropriate to the sensitivity of the data those systems are expected to handle, manage and store; external storage and processing (i.e., cloud resources or applications) must be security assessed or tested prior to approval for use.	OT25-7 The Company does not allow cyber-enabled systems that control, monitor, or record data from physical security systems to reside on the same control networks as the physical security systems. OT25-8 The Company requires that any special-purpose test equipment or maintenance equipment or systems put in place for maintenance, prototyping or system development be removed at the conclusion of the event, particularly if the equipment presents communications or interface capabilities that are not documented in the FDD. OT25-9 The Company requires databases that interface with web servers or web data sources within the OT/ICS segment(s) to be inaccessible to the Internet. OT25-10 The Company requires that no administrative functions from general-purpose networks (mail, etc.) be available on OT/ICS or process control systems or interface systems, appliances or devices. OT25-11 The Company requires that systems not requiring continuous wireless connectivity must be scheduled and managed for connections, and not left connected by default.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		IT25-8 The Company plans and implements distributed network monitoring infrastructure, using load distribution methods and tools as required to confirm collection systems cannot be overloaded. IT25-9 The Company requires that any special-purpose test equipment or maintenance equipment or systems put in place for networked system maintenance, prototyping or system development be removed at the conclusion of the event, particularly if the equipment presents communications or interface capabilities that are not documented as network resource capabilities.	
(26) Provide Secure Engineering ***Best Practices Include*** *The Company architects, designs, and builds systems and processes with monitoring and security or performance measurement in mind.* *The Company installs systems on its networks with pre-defined, approved security hardening configurations that minimize the potential for unexpected vulnerabilities.* *The Company secures its communications paths through commercial providers' networks by encrypting their communications paths and data transmissions to and from critical systems and functions.* *The Company manages encryption methods and cryptography suites used to maintain currency with industry standards, personnel skills and capabilities to manage, and supportability for chosen standards through the security architecture.* *The Company architects protective devices between information technology networks and operational technology networks to limit traffic types, protocols and origins, and to trace and log all traffic into the operational technology network(s).*	***Process Specification Requirement*** P26-1 The Company requires all systems acquired, procured or built for the enterprise shall meet all minimum requirements for security and effective integration and interoperability with the architecture. P26-2 The Company requires systems management communications for servers, systems or appliances to be performed via encrypted means, e.g., Secure Shell (SSH), and encryption keys must be managed on systems separate from the administrator machines and credentials used to access the systems. P26-3 The Company requires new systems or projects to support continuous monitoring and performance monitoring in order to provide application or system visibility for network monitoring systems. P26-4 The Company exercises architectural governance over networked resources by periodic review of network structures and architecture as built, taking opportunities to rationalize and consolidate networks in order to confirm consistent and universal security is maintained throughout the enterprise.	***Information Technology Specification Requirements*** IT26-1 The Company requires all systems projects shall use enterprise solutions for inherited services and security controls within the networked environment. Required inherited functions and controls include: 1. Boundary defense and perimeter protections; 2. Application and data hosting methods and resources; 3. Virtual Private Network (VPN) connection methods and destinations; 4. User authentication methods (through Active Directory); 5. Privileged access controls through escrowed password storage; 6. Data transmission paths, using enterprise contract-provided resources only; 7. Domain Name Service; 8. Data encryption methods; and 9. Patching and patch management methods that maintain configuration control and change controls throughout the enterprise. IT26-2 The Company prohibits use of web servers on end user systems or endpoints without specific authorization and security configurations in place.	***Operational Technology Specification Requirements*** OT26-1 The Company requires sensors that report on web protocols, and the servers which will aggregate their data, to be tested for both security and functional data integrity prior to be placed in service. OT26-2 The Company requires sensors and systems reporting on web protocols to servers or aggregator devices to only provide data on secure protocols, with all insecure ports and protocols closed or disabled, unless specifically authorized and implemented with compensating controls. OT26-3 The Company restricts and filters communications from IT-based control systems to operational and process technology (OT) systems so as to confirm that access authentication and verification processes occur outside of OT system software and appliances. OT26-4 The Company develops, engineers and builds OT/ICS that support management automation and sensor management or monitoring, including performance monitoring.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company installs peripherals on its networks with pre-defined, approved security hardening configurations that remove web and wireless network servers and protocols prior to connection to the network. *The Company specifically authorizes, and limits operational protocols to, those protocols needed on the network for business-critical requirements.* *The Company terminates all VPNs outside the boundaries of any critical systems or components, and at nodes that are monitored for access and activity.* *The Company provides protective screening and filtering of VPN-borne traffic to prevent malware on remotely-connected systems from transiting the VPN into the main networked systems without passing through a security monitoring package.* *The Company uses secure maintenance methods that include limits on what computer-based maintenance assist or analysis gear can be used for, and with what systems; how systems will be patched and updated (in accordance with prior change control practices); and how maintenance personnel on cyber-enabled systems will be trained and certified to recognize signs of reportable abnormalities, anomalies and exceptions that may indicate safety and security issues.*	P26-5 The Company uses secure maintenance methods that include limits on what computer-based maintenance assist or analysis gear can be used for, and with what systems; how systems will be patched and updated (in accordance with prior change control practices); and how maintenance personnel on cyber-enabled systems will be trained and certified to recognize signs of reportable abnormalities, anomalies and exceptions that may indicate safety and security issues. P26-6 The Company requires that any project, system, application or appliance to be implemented in the network, with interfaces to other systems, present interface documentation prior to installation or integration.	IT26-3 The Company requires all new systems or projects to be implemented with encrypted authentication mechanisms (i.e., no clear text passwords passed through the network). IT26-4 The Company specifically authorizes, and limits operational protocols to, those protocols needed on the network for business-critical requirements. IT26-5 The Company implements and uses a demilitarized zone (DMZ) to segregate outside access systems and network segments from the internal segments of the network. IT26-6 The Company installs peripherals and utility devices on its networks with pre-defined, approved security hardening configurations implemented prior to installation on the network. IT26-7 The Company terminates VPNs or remote access authentication systems outside the boundary of any critical systems or components to confirm accountability of access through separate and discrete login or logoff procedures. IT26-8 The Company secures its communications paths through commercial providers' networks by encrypting their communications paths and data transmissions to and from critical systems and functions. IT26-9 The Company manages encryption methods and cryptography suites used to maintain currency with industry standards, personnel skills and capabilities to manage, and supportability for chosen standards through the security architecture.	

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
2- Risk Understanding and Management			
(27) Exercise Penetration Testing ***Best Practices Include*** *The Company uses penetration testing to determine the effectiveness of their protective systems and process controls by testing the enterprise technical systems against adversary-like methods.* *The Company applies best practices for system hardening prior to penetration testing, using the test to show discrepancies and gaps, rather than expecting the test to show the entire requirement for hardening.* *The Company uses penetration testing results to generate an action list that can inform the capital development plan for budgeting security improvements.*	***Process Specification Requirement*** P27-1 The Company exercises a regular schedule of penetration testing to check effective security, show gaps or assumptions in operational systems, and indicate where resilience of engineered systems may be fragile. P27-2 The Company uses its own tools to assess its conditions prior to undergoing outside assessment or test, allowing technology personnel to eliminate common vulnerabilities prior to the test. P27-3 The Company uses strict rules of engagement to structure and plan penetration tests to confirm the tests cannot cause inadvertent damage or harm to systems or facilities under test, and nor shall the tests be allowed to proceed to the point of causing safety violations or environmental impacts. P27-4 The Company links penetration testing to application and system security testing, gauging the effectiveness of software or system security tests with the degree of resistance those applications or systems demonstrate under adversarial testing.	***Information Technology Specification Requirements*** IT27-1 The Company shapes penetration tests in ways that allow internal technology staff to learn as much as possible about their systems and potential weaknesses in those systems. IT27-2 The Company conducts penetration tests that treat the Company as would enterprise threat actors, using threat tactics, techniques and procedures (TTPs) as much as can be replicated during testing. IT27-3 The Company confirms testing teams assess all aspects of public-facing systems, using expected penetration or exploitation tools against outward-facing enterprise systems. IT27-4 The Company uses penetration testing results to map potential shortfalls in threat intelligence with risk assessment or management processes, in order to improve understanding of weak areas and to advance protective control requirements in areas found deficient. IT27-5 The Company provides briefings and after-action reports to executive leadership as security progress measures, and to reinforce capital planning requirements for security and secure engineering needs.	***Operational Technology Specification Requirements*** OT27-1 The Company uses the Functional Description Document (FDD) to help structure periodic penetration tests against potentially vulnerable components, systems or interfaces in the enterprise's functional OT/ICS. OT27-2 The Company performs OT/ICS penetration tests to determine potential gaps in protective system or control coverage, and to help develop both technical and non-technical control measures to apply against shortfalls. OT27-3 The Company performs OT/ICS penetration testing to confirm expectations of safety and system Integrity Levels, and the access limits or parameters that must always be protected because those limits are where systems may suffer functional effects of unauthorized contact, intrusion or attack.
(28) Build Forensic Analysis ***Best Practices Include*** *The Company builds and maintains forensic analysis skills, tools and procedures to enable technology personnel the appropriate foundation and abilities to execute forensic evidence gathering and forensic analysis, both to satisfy malware or intrusion-related forensic analysis, and to assist in Legal or HR-related investigatory activities.*	***Process Specification Requirement*** P28-1 The Company maintains the tools and methods necessary to conduct evidence gathering and forensic analysis, and the personnel skills needed to exercise forensic procedures. P28-2 The Company promulgates a policy and procedures for conducting forensic evidence capture and analysis, including Legal, Human Resources and Privacy departments' involvement, in addition to the technical data gathering activities conducted by technology or system personnel.	***Information Technology Specification Requirements*** IT28-1 The Company logs, retains and reviews all access attempts within an organizationally-determined period of time in order to perform incident response process and forensics as required. IT28-2 The Company's Incident Response Plan, when executed, enables evidence gathering for forensic analysis, and the procedures for evidence capture are trained with IR procedures.	***Operational Technology Specification Requirements*** OT28-1 The Company's OT/ICS Incident Response and Continuity Plan (IRCP), which contains recovery action plans for reestablishing normal safe operating conditions of the impacted personnel, systems, ship/ platform/ facility, including a plan for recovery from any detrimental environmental impacts, provides all evidence and retention to enable forensic investigation.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company structures forensic activities under enterprise policy to include specifically the Legal, Human Resources and Privacy departments for their collaborative roles in forensic evidence gathering. *The Company links specific objectives under security continuous monitoring activities to forensic activities and processes, the better to confirm indicators of attack or indicators of compromise are preserved for forensic and damage analyses.*	P28-3 The Company scopes functional system incident response to the criticality of components or systems suffering failure, intrusion or attack, using Integrity Level (IL) categorizations and criticality to personnel, environment, facility or system safety to determine response, communications plan, emergency actions, etc. P28-4 The Company provides appropriate working spaces, safe storage, directed authority and guidelines for evidence capture, procedures to safeguard evidence, and equipment or applications to aid in evidence gathering and safeguarding.	IT28-3 The Company uses Perimeter Protections, Security Continuous Monitoring and Incident Response activities, both daily and situational, to provide the logs and records necessary to understand and track incidents, using indicators of attack, Internet Protocol addresses, domain names, email addresses, or Uniform Resource Locators (URLs) observed in log data to correlate against indicators of compromise in threat intelligence data.	OT28-2 The Company assigns and documents a "level of severity" and "type" designation (e.g., successful breach, attempted-but-failed breach, suspected breach attempt, and suspicious or unauthorized activity) to each incident to direct proper forensic response. OT28-3 The Company logs, retains and reviews all access attempts within an organizationally-determined period of time in order to perform incident response process and forensics as required. OT28-4 The Company logs and reviews all remote login attempts, recording all available contextual data (i.e., record the time, date, duration, and source of all remote access events, and record and document unsuccessful attempts (suspected probes) at remote access.)
(29) Enforce Privacy Data Management ***Best Practices Include*** *The Company understands its legal, regulatory, policy and guidelines environment for the geographic areas or nations in which it operates, and it safeguards personnel data to the strictest standards required by the most stringent compliance requirements.* *The Company segregates personnel and privacy-related data away from other, less-critical data, to reduce the potential for breaches to enterprise data including privacy-related data.* *The Company vets personnel with access to privacy-related data, and it limits access to those personnel and no others.* *The Company appoints an official with technical knowledge of networked systems to be in charge of privacy-related data and issues therein.*	***Process Specification Requirement*** P29-1 The Company uses End User Notice and Consent forms for any personal data gathered on enterprise systems, including both internal-facing and external-facing systems and websites. P29-2 The Company uses periodic internal checks of privacy-related data management and handling procedures to self-assess compliance with regulatory requirements for applicable geographic areas. P29-3 The Company assesses potential gaps or shortfalls in privacy-related data handling procedures and feeds this information directly to capital planning, governance and audit oversight processes for priority handling. P29-4 The Company requires that personnel data that must be gathered be collected from employees with 1. Notice of purpose; 2. Choice to provide, with indications or impact for failure to provide; 3. Purpose limitations in consonance with notice and choice;	***Information Technology Specification Requirements*** IT29-1 The Company keeps data gathered from its websites (employee or customer/member data, or website visitor data) segregated from the data served on the website(s) to prevent inadvertent mixing of potential privacy-related data with other data. IT29-2 The Company requires any application in the networked environment to encrypt its data stream when gathering, transmitting and storing privacy-related data from employees or other personnel. IT29-3 The Company treats any data that can show personnel location, personnel activities, or personally-identifiable information (PII) as special-category data to be safeguarded with very strict access control applied. IT29-4 The Company monitors potential data capture points in the enterprise for any anomalous or unauthorized connections in the physical architecture.	***Operational Technology Specification Requirements*** OT29-1 The Company determines specific data events or flows, where applicable, that may reflect personnel location, personnel activities, or personally-identifiable information (PII) in OT/ICS operations and monitoring, and records those events or flows as special-category data in the Functional Description Document (FDD) to be safeguarded with very strict access control applied.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	4. Recourse against loss or compromise, with enforcement provisions. 5. Accountability for further transfer outside the boundary of the collecting organization; 6. Security against loss; and 7. Data integrity in storage and transit. P29-5 The Company collects geographic and activity-related data, system and application access data, and website resource access data by employees and other network users for purposes of network security; this data is governed by policy so as to only become personnel activity data (i.e., potential PII) with active involvement of both Legal and HR.	IT29-5 The Company considers both the known locations for PII and the potential locations of PII in networked resources, and it confirms backup and archive file sets from those network segments, areas, regions or systems are protected in accordance with compliance regulations. IT29-6 The Company uses active data monitoring methods (i.e., network sniffing) to verify that PII or other privacy-related data is encrypted if or when it is transmitted through the network.	
(30) Provide Mobile Data Management ***Best Practices Include*** *The Company understands its legal, regulatory, policy and guidelines environment for the geographic areas or nations in which it operates, and it safeguards personnel and mobile data to the strictest standards required by the most stringent compliance requirements.* *The Company implements a Mobile Data Management (MDM) program that can meter, monitor and control enterprise data content on mobile devices enrolled in the program.* *The Company requires employees with any mobile device (phone, tablet, non-enterprise laptop, reporting sensor, etc.) to enroll in the MDM program prior to receiving enterprise data access through the device.* *The Company has, promulgates and trains employees on a formal device management policy that covers correct use and access of enterprise resources by portable devices.*	***Process Specification Requirement*** P30-1 The Company uses written notifications and policies to confirm employees understand and acknowledge the capabilities and limitations they are granted for placing enterprise data on either enterprise or personal mobile assets. P30-2 The Company governs and tracks all mobile devices through Mobile Device Management (MDM) methods and technical means for phones and tablets, and through network inventory control for mobile appliances, laptops and other computational equipment. P30-3 The Company's employees may be allowed to operate under a Bring-Your-Own-Device (BYOD) policy in some cases. a. Departments allowing BYOD usage shall consider business or mission requirements for mobile devices, including work culture, usage patterns, and any applicable legal issues that may apply to use of employee-owned devices in conducting work activities with such devices. ***b.*** Users of employee-owned devices under the BYOD program shall	***Information Technology Specification Requirements*** IT30-1 The Company defines the types of enterprise data which can be used or stored on portable devices, the conditions for which it may be used, and the duration of use during which it may be retained on the portable device. IT30-2 The Company uses MDM methods and technical means to protect Company data on mobile devices, including to destroy all data on devices that are lost, stolen or removed from Company employee custody. IT30-3 The Company uses security continuous monitoring technical methods to observe enterprise systems that connect to portable devices, scanning for malware that may be introduced from those portable devices. IT30-4 The Company defines and enforces the types and conditions for connections between portable devices and enterprise systems, including physical or virtual ports allowed for use; approved software link mechanisms and applications; and conditions under which portable devices may store enterprise data or act as data transfer devices.	***Operational Technology Specification Requirements*** OT30-1 The Company defines those conditions under which remote access via portable devices, including phones, tablets, laptops or devices, will be allowed, and what minimum standards for connectivity to OT or process control systems are required prior to connection. OT30-2 The Company defines very strictly and documents those conditions and procedures under which remote access to OT/ICS may be accomplished via mobile devices. OT30-3 The Company monitors remote access accounts allowed mobile device access, and anomalous behavior or reports of device theft or misuse trigger immediate termination of that device's remote access. OT30-4 The Company uses posted policies and enforcement controls (e.g., storage lockers) to regulate use of cell phones and mobile devices in OT/ICS spaces; during special security events, such as software loads; and during times when electronic signals may interfere with OT/ICS functions or control mechanisms.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	i. Enroll in the Company's mobile data management (MDM) program prior to receiving Company enterprise mail or data on their devices; ii. Consent to enrollment in MDM through written agreement filed with HR; and iii. Only have access to specific time-limited durations of mail or data on their devices (period depends upon policy and applicability). P30-4 The Company uses posted policies and enforcement controls (e.g., storage lockers) to regulate use of cell phones and mobile devices in organizational spaces and during organizational events requiring special security measures.		OT30-5 The Company uses posted policies and enforcement controls to regulate or limit the use of photography around OT/ICS components, systems or appliances; critical control systems; or OT/ICS infrastructure. OT30-6 The Company defines and enforces the types and conditions for connections between portable devices and enterprise OT/ICS, including physical or virtual ports allowed for use, and for what uses; any approved software link mechanisms and applications; and conditions under which portable devices may store enterprise data or act as data transfer devices.
(31) Provide Certificate Management ***Best Practices Include*** *The Company uses cryptographic certificates to authenticate personnel, systems, messaging, portable devices, sensors and other enterprise systems to provide accountable and non-repudiable methods for granting access to enterprise systems and data.* *The Company manages cryptographic certificates across the enterprise with a management system that matches personnel, devices, certificates, issue and expiry dates, certificate originator, and other data as required.*	***Process Specification Requirement*** P31-1 The Company enables use of cryptographic certificates in web-based systems by enabling 'https everywhere' on servers and in employee browsers. P31-2 The Company uses certificate-based signing capabilities in email and messaging to confirm employee email can be authenticated to specific personnel, and to differentiate from spoofed or fraudulent emails. P31-3 The Company uses an external Certificate Authority for its certificates used with external communications, but it may establish and use an internal Certificate Authority for self-signed certificates in internal communications. P31-4 The Company uses keys of length sufficient to protect communications, but within the computational resource limits of enterprise-standard devices to use and manage. P31-5 The Company conducts periodic internal audits of certificate chains to confirm all certificates install and reference correctly, and that chains of trust are intact within the enterprise.	***Information Technology Specification Requirements*** IT31-1 The Company uses public key infrastructure (PKI) technology and certificates to confirm email can be authenticated to individual users. IT31-2 The Company provides browser applications that support cryptographic certificates across the enterprise, and it restricts browser plug-ins or helper modules to those that have been tested and approved for use in the enterprise. IT31-3 The Company generates and tracks an inventory of user certificates and internal application or server certificates that support the Company. IT31-4 The Company tracks, renews and replaces expired certificates in all systems, servers and endpoints and browsers before they can cause service outages. IT31-5 The Company configures and requires internal domains to support encrypted communications paths (i.e., https) on internal communications lines.	***Operational Technology Specification Requirements*** OT31-1 The Company uses certificates on authorized portable devices to assist in authenticating authorized users in performing remote access from those devices.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P31-6 The Company chooses cipher suites and key lengths for internal encryption to match (1) risk factors from potential traffic interception; (2) computational resource limits (i.e., long keys are more secure but can slow computers considerably), (3) export restrictions and requirements to operate in overseas locations where such export restrictions may affect choices. P31-7 The Company requires every IT project to include cryptographic functions as part of basic system capabilities, including enterprise-standard methods for certificate and key management.	IT31-6 The Company protects private keys in accordance with a standardized method that is distributed and trained to all employees; private keys are only kept on secure and trusted machines, and private keys are regenerated when personnel changes occur. IT31-7 The Company confirms that administrators are subject to separation of duties checks and restrictions to prevent an administrator who generates encryption keys from being able to access the data encrypted with those keys. IT31-8 The Company confirms the protocols used in enterprise systems are tracked and kept updated and current, with enterprise-wide patching taking a priority for Transmission Layer Security (TLS). Conversely, deprecated or compromised encryption suites with vulnerabilities or weaknesses shall be expeditiously removed from the enterprise. IT31-9 The Company includes enterprise-wide certificate management as a contingency procedure in its Incident Response Plan, in event of a Certificate Authority or encryption algorithm compromise.	
(32) Exercise Communications Management ***Best Practices Include*** *The Company limits its total connections to the Internet to planned, finite numbers that can be easily managed, accounted, and audited, and each of which can be screened through security appliances and systems.* *The Company secures its communications paths through contract terms with providers to maintain reliability and security of communications functions.* *The Company will run periodic inventories against its contracts and technical architecture, verifying its external connections to the Internet and to other transmission paths.*	***Process Specification Requirement*** P32-1 The Company manages telecommunications systems connections to provide simplicity and fault tolerance in case of transmission line loss, managing telecommunications contract terms for service level agreements and connection prioritization. P32-2 The Company confirms that all enterprise communications that pass from long-haul providers to local providers (i.e., "last mile") are encrypted by enterprise infrastructure systems to prevent easy intercept at the systems interfaces. P32-3 The Company plans fault tolerance into its systems, applications and utilities to confirm that loss of communications to a system, asset, platform, or ship system cannot cause a safety issue to occur.	***Information Technology Specification Requirements*** IT32-1 The Company develops, designs, builds or contracts for systems that can withstand loss of communications or data transmission without causing safety issues for personnel, the environment, the asset or system(s). IT32-2 The Company requires communications, routing and switching infrastructure components to be configured and operated to provide encrypted data throughout the network. IT32-3 The Company provides secure communications channels in out-of-band methods to support incident response, as necessary.	***Operational Technology Specification Requirements*** OT32-1 The Company maintains current communications paths and protocols in diagrams and artifacts in the Functional Description Document (FDD). OT32-2 The Company screens communications paths and messaging (i.e., email, social messaging) prior to delivery into proprietary networks in order to detect and eliminate potentially corruptive files, attachments, and links. OT32-3 The Company actively secures data networks that connect its classified assets or transfers classified data, with special consideration given to assets that are in geographically remote or difficult to reach locations.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company verifies its communications paths between and among assets, systems and facilities support data protection methods (i.e., encryption) and technical performance auditing and monitoring.		IT32-4 The Company provides segmentation around functional areas of the network by use of infrastructure device architecture and configuration, to protect specific areas of the network and enterprise assets.	OT32-4 The Company restricts and filters all communications from IT-based control systems to operational and process technology (OT) systems so as to confirm that access authentication and verification processes occur outside of OT system software and appliances. OT32-5 The Company uses unidirectional network technology (e.g., an optical data diode or similar) on outgoing data reporting networks/ mechanisms to prevent unauthorized incoming communications with critical components or systems. OT32-6 The Company's security architecture provides for implementation of protective devices between information technology networks and operational technology networks in order to trace and log all traffic, limit traffic types, traffic protocols, and traffic origins. OT32-7 The Company does not allow cyber-enabled systems that control, monitor, or record data from physical security systems to reside on the same control networks as the physical security systems. OT32-8 The Company segregates networks supporting emergency backup processes and systems that are frequently associated with safety and shutdown capabilities from operational or mission critical system networks.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
3- Protected Resources and Accesses			
(33) Enforce Network Access Control ***Best Practices Include*** *The Company restricts endpoint or device access based on authenticated entry and device or system compliance with the enterprise security policy.* *The Company uses network access control as a means to direct personnel or systems to the network resources to which they have been granted access by their roles or identity attributes.*	***Process Specification Requirement*** P33-1 The Company uses network access control (NAC) technical methods to enforce uniform enterprise system policies and hygiene across all access points, including conventional networks, virtual private networks (VPNs) and wireless networks. P33-2 The Company uses NAC to complement unified identity management processes and to assign users to their appropriate network resources by their roles and identity attributes.	***Information Technology Specification Requirements*** IT33-1 The Company uses NAC to report compliance with enterprise cyber hygiene rules prior to network entry, placing non-compliance machines in limited-access virtual local area networks (VLANs) until their hygiene issues are corrected. IT33-2 The Company uses NAC to scan and authorize machines or systems joining the conventional network, and those joining remotely, over virtual private network (VPN). IT33-3 The Company requires NAC to report anomalous behaviors of users if they move from their authorized network resource locations to other areas of the network. IT33-4 The Company uses NAC in combination with network security appliances and systems to monitor outgoing communications from scanned endpoints, removing and isolating machines showing signs of malware or unauthorized communications.	***Operational Technology Specification Requirements*** OT33-1 The Company manages connections to the OT/ICS from authorized, dedicated ICS devices with Change Management controls to deploy approved changes to any ICS infrastructure as needed (PLCs, SBCs, etc.).
(34) Enforce Third Party Access Management ***Best Practices Include*** *The Company takes precautions for third party (outside) access to enterprise resources in order to establish evidence-based trust and systemic monitoring to verify ongoing trust as the third party is granted access to data and systems.* *The Company performs due diligence audits, or uses professional auditors' reports, on the third party vendors, suppliers, or contractors to whom they will grant access to enterprise data, systems and network resources.* *The Company confirms access to systems, data and network resources is addressed in contracts between the parties.*	*Process Specification Requirement* P34-1 The Company uses well-defined processes for vetting third-party personnel and computers that are credentialed for access to proprietary networked resources. P34-2 Access management to Company network resources by third parties shall be governed under rules formulated for appropriate groups within the organization, to include a. Employees b. Consultants c. Contractors – on site d. Contractors – off site e. Vendors and suppliers f. Business partners and joint ventures g. Subordinate organizations within the enterprise h. Cloud service providers	***Information Technology Specification Requirements*** IT34-1 The Company uses written notifications and policies to confirm third-party personnel understand and acknowledge the capabilities and limitations they are granted for placing enterprise data on either enterprise or personal mobile assets. IT34-2 The Company uses well-defined processes for vetting third-party personnel and computers that are credentialed for access to proprietary networked resources.	***Operational Technology Specification Requirements*** OT34-1 The Company provides positive action to manage a need-based subcontractor access program to facilitate authorized access to offshore or marine ICS assets. OT34-2 The Company defines performance, organizational, and security related requirements when contracting with third-party data management service providers and software applications providers. OT34-3 The Company requires third-party personnel to access enterprise OT/ICS to receive training in systems safety, software management of change requirements, access protections, password strength, and two-factor/ multi-factor authentication methods prior to being allowed to work on OT/ICS.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
The Company confirms access to systems, data and network resources is both monitorable and actively monitored for anomalous behaviors and exceptions to policy.	P34-3 The Company's acceptable use polices clearly communicate tips and methods concerning cybersecurity "hygiene" to (as appropriate) contractors, suppliers, and customers through periodic training containing tips and methods for maintaining a functional technology. P34-4 The Company confirms technology provisioning and service contracts are reviewed by appropriate security personnel, with third parties providing audit reports and information as necessary for the Company's vetting process. P34-5 The Company confirms that work performed on networked resources by third parties is inspected and approved prior to acceptance; that no intermediate work or equipment is left behind that could provide unmonitored access to the network; and that third party access credentials are terminated as soon as their personnel meet all contractual obligations. P34-6 The Company reviews all procurement contracts for supply chain risk issues if critical components or systems may be procured from layered contracts with no discernable chain of custody for those components or systems. P34-7 The Company reviews all cloud application service contracts to determine contractual responsibility, accountability and liability for sensitive data losses, if the service provider is not in complete control of their own service systems. P34-8 The Company devises and uses measures and metrics to integrate the vulnerabilities created by third parties in the enterprise supply chain with the enterprise risk management program. P34-9 The Company includes service-level agreements (SLAs) governing third party access to enterprise resources in its contracts, defining expectations of contractors, expectations for access, and monitoring or management of that access.	IT34-3 The Company defines third party access via virtual private network (VPN) as including system protective restrictions on minimum security baseline on third-party machine(s); limits on account duration; limits on connection duration; limits on account access scope; and limits on how much data is retained by the third party, of what type, and where. IT34-4 The Company defines and inspects to standards for any third party machine that will connect to the enterprise networks or access network assets. IT34-5 The Company actively seeks positive procurement contract terms indicating vetting and attestation by the manufacturer or supplier of all hardware provided under the contract(s). IT34-6 The Company actively seeks positive procurement contract terms indicating attribution by the manufacturer or supplier of all software and licenses included on computer-based systems provided under the contract(s). IT34-7 The Company requires that authorized third party personnel use strong passwords and two-factor authentication for connection to proprietary networked systems. IT34-8 The Company requires that guest users who access proprietary network resources use traceable Company-provided login credentials. IT34-9 The Company requires third-party developers or system development houses working with the Company for internal development projects, programs, and technology personnel shall follow standard security guidelines associated with corporate policies. 1- Permissions to reach production servers is strictly controlled and outside the limits of access for any developers.	OT34-4 The Company designates a local (onboard) authority to be responsible for monitoring subcontractor compliance to all OT/ICS security policies and procedures; the local authority may authorize or revoke any or all of a subcontractor's access to the ICS. OT34-5 The Company and its local monitoring authority personnel prohibit subcontractor access to the ICS without authorization (permission) from the local authority (e.g. permit to work, work authorization form, etc.). OT34-6 The Company and its local monitoring authority personnel develop and maintain a local (onboard) ICS subcontractor access record containing time of access, name of accessing person, or corporate ID of accessing person. OT34-7 The Company and its ICS Security Office, Corporate Safety Office, and on-asset supervisors will collaborate to establish and document physical access permission methods (e.g., keys, physical tokens, passwords, door lock combinations, etc.) and access logging methods based on approved on-asset operational logic. Document control perimeters in the FDD.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		2- No development agent shall have access to development tools and administrative rights without proper training on the systems in question. 3- No single agent may be allowed accesses which could result in destruction of data without controls and safeguards in place to recover from errors. 4- Address scope given to developers or development houses will be consciously restricted to what the development effort requires. Each development effort shall be reassessed for address space and access as required. 5- Individual developers shall use personally-identifiable accounts to confirm their activities are traceable within enterprise systems and networks, consistent with all users within the enterprise environment. 6- Developers' machines shall not connect directly to the COMPANY enterprise network without protective, or prophylactic, screening devices between the environments. Developers may be given access to remote desktop environments, or they may have remote access to machines within the COMPANY enterprise. 7- Developers shall not have access to Remote Desktop Protocol (RDP) file transfer without specific authorization and carefully scoped permissions. Use of RDP shall be monitored closely to prevent unexpected data exfiltration.	

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
(35) Implement Secure Software Development ***Best Practices Include*** *The Company requires its development organizations to use secure software development techniques and methods when generating software or firmware for any system, application so device in the enterprise.* *The Company uses technical software testing methods and techniques to verify its software meets enterprise and/or external customer compliance requirements.* *The Company introduces security requirements and constraints into the development process as early as practicable, ensuring the security and engineering or development teams work together to reduce and remove software risks to the Company.* *The Company standardizes and requires usage of enterprise security services to be used across all possible applications and systems, including such functions as network authentication, authorization for access, federated authentication for third parties, and network access via virtual private network (VPN).* *The Company safeguards software code as Intellectual Property (IP) that is due appropriate safety against loss or theft, as would physical property.* *The Company confirms that development is conducted in supportable, modern languages, in modules or partitions that enable useful technical reviews and code walkthroughs.*	***Process Specification Requirement*** P35-1 The Company develops and promulgates policy and specific procedures for secure software development requirements for all enterprise software. P35-2 The Company tracks dependencies across the enterprise applications (libraries, common sources, common data, hierarchical resource requirements, common databases, etc.) to confirm the application portfolio is managed holistically. P35-3 The Company assesses potential threats and attendant enterprise risks associated with specific applications or systems developed in or for the Company, and it requires integration of mitigation measures to such threats or risk conditions during code development. P35-4 The Company uses industry best practices for secure coding to increase security and quality of code components, systems and applications, including but not limited to: • Input validation; • Testing against common application insecurity methods; • Strong authentication requirements; • Architectural separation of applications and databases; • Signed code; and • Updates on pull, not push. P35-5 The Company requires software to protect user credentials and prevent credential capture or theft. P35-6 The Company requires all software to enforce end user access controls, either mandatory or discretionary, in mechanisms that allow the enterprise to restrict and monitor data accessed by software users.	***Information Technology Specification Requirements*** IT35-1 The Company uses a security development lifecycle approach to software development, including security functions and enterprise security requirements at the developmental stages most appropriate to accept those system requirements, resulting in a security feature-complete application or system at the completion of the development cycle. IT35-2 The Company manages software through its lifecycle for security functions and security vulnerabilities, tracking reported security issues as priority mitigation requirements in the quality assurance of the product(s). IT35-3 The Company is strict in requiring testing and configuration control of updates and version changes to developmental modules or components used in software being developed. IT35-4 The Company performs code walk-throughs as part of its technical review process, ensuring its development team and engineering leadership understand the functional architecture, system or code dependencies, and functional security being implemented, in time to make changes prior to delivery to either internal or external customers. IT35-5 The Company understands and implements all licensing associated with the software it is developing, any third-party components it is using, and any outside requirements imposed for end-user environment or context. IT35-6 The Company tracks third-party source code used in software development to understand potential areas of vulnerability or dependency introduced by use of the outside libraries, functions or resources.	***Operational Technology Specification Requirements*** OT35-1 The Company adheres to accepted enterprise-standard and industry-standard software engineering development practices in requirements for acquisition, changes, and removal of ICS-supporting software. OT35-2 The Company compiles and maintains a revision-controlled Functional Description Document (FDD) that contains information about enterprise systems, their software, technical details of that software, vulnerabilities and patches reported/ received / installed for that software.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P35-7 The Company prioritizes testing and remediation tasks that align with enterprise risks and organizational strategies. P35-8 The Company provides resources in development projects that aim specifically to prevent the most likely and most harmful types of malfunction, intrusion, breach or attack, especially in those applications that process or transfer privacy-related data. P35-9 The Company structures its development and security testing processes to identify functional areas requiring additional emphasis, and then using this data to show progress toward organizational goals in software quality and security. P35-10 The Company monitors trouble reports, test results and help desk tickets on software and the enterprise software portfolio to understand the enterprise risk posture, using compiled results for governance decisions regarding allocation of investment to reduce security or functional risks. P35-11 The Company uses threat intelligence and community threat information and best practices to inform its developers, user community and executive leadership about the security requirements necessitated by known (or suspected) threat sources. P35-12 The Company includes security personnel in code reviews, milestones, progress reports and walk-throughs. P35-13 The Company requires that software applications or systems avoid use of insecure protocols without specific dispensation from the Company, as verified through ST&E processes. P35-14 The Company requires any software or system released either inside or outside the enterprise meets strict standards for documentation, security and operability to confirm released software poses no threat, legal or logical, to the enterprise as a result of unexpected behaviors.	IT35-7 The Company uses firewalls or protective screening systems to prevent developmental software from using external package repositories accessed from either development environment or production environment servers, in order to prevent dynamic includes from being used in the final software. IT35-8 The Company carefully considers use of any external libraries in enterprise applications prior to authorizing their use; loss of communications links may cause malfunction of applications with those external dependencies. IT35-9 The Company performs threat modeling of applications and systems, including data flows and architecture/design, become important parts of the development lifecycle. IT35-10 The Company limits use of cloud service application programming interfaces (APIs) that have accessibility from the open Internet. IT35-11 The Company confirms that software code repositories are closely managed, carefully restricted for personnel access, and strictly limited in avenues of logical access through any network, with accountability for any access event. IT35-12 The Company conducts ST&E in the same developmental phase as alpha testing; no software may be distributed outside the enterprise (i.e., to customers for early experience testing) without security testing completed first. IT35-13 The Company requires that code under test be afforded the same protections as code under development, with access by personnel, machines and all logical means restricted to required accesses and methods only.	

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
		IT35-14 The Company actively manages access to code under either development or test by third parties, e.g., contracted development houses, and such access is metered and monitored by the Company, and governed under strict contractual terms between the parties. Machines at the third party development house with access to code repositories are to be limited in their abilities to store or transfer data locally. IT35-15 The Company requires any machine with access to code repositories to have no: (1) operable USB ports, (2) writable optical disk drives; (3) access to any shared drive outside the development environment; and (4) access to cloud or external services to which code or files may be transferred.	
(36) Execute Security Test & Evaluation ***Best Practices Include*** *The Company uses Security Test and Evaluation (ST&E) for all software applications and development projects, ensuring build and/or installation meet enterprise security requirements.* *The Company uses ST&E to identify and mitigate enterprise risk conditions or challenges,* *The Company maintains and uses a security testbed for all ST&E activities, providing a representative environment for testing of software prior to deployment to operational ships, platforms, assets or facilities.* *The Company uses ST&E test resources as an enterprise asset, documenting and maintaining the asset set as any other enterprise asset would require for configuration control, system training, periodic maintenance and upkeep, etc.*	***Process Specification Requirement*** P36-1 The Company develops and promulgates policy and specific procedures for security test and evaluation (ST&E) of developmental, packaged (commercial), open source and all other software, per enterprise requirements for security development and risk management. P36-2 The Company performs ST&E of all projects, programs, applications, systems and appliances that connect to the enterprise networks, systems or repositories including review, test and approval by organizational security personnel prior to deployment and activation of such projects, systems, etc. on the production network. P36-3 The Company tests for dependencies across the enterprise applications (libraries, common sources, common data, hierarchical resource requirements, common databases, etc.) to confirm the application portfolio is managed holistically, and that risks that can arise from such dependencies are accounted and managed.	***Information Technology Specification Requirements*** IT36-1 The Company tests all software (developmental, packaged, open source and all other as applicable within license agreements) for unexpected behaviors prior to being placed on the network; unexpected and undesired behaviors include establishing covert channels; using undocumented ports; providing undocumented (backdoor) access; capturing and transmitting data without operator permission, or other behaviors as determined undesired by the Company. IT36-2 The Company provides test results and reports from ST&E process to project managers or vendors for them to build appropriate risk mitigation plans for their software products. IT36-3 The Company evaluates application programming interfaces (APIs) as part of security test and evaluation of applications or software-intensive systems, as unknown risks may accrue from third-party APIs with weak interfaces or poor security implementations.	***Operational Technology Specification Requirements*** OT36-1 The Company performs security testing against OT/ICS software and systems installations to determine potential security problems that may be addressed with external screening, segmentation, proxy installation, or with other technical or non-technical means that do not require modification of the OT/ICS itself. OT36-2 The Company tracks all OT/ICS software components which have security test and evaluation (ST&E) discrepancies as a result of inherited enterprise issues, i.e., downstream or host system present vulnerabilities that affect the OT/ICS, as OT Technical Debt to be addressed in governance and capital planning. OT36-3 The Company requires all applications or software products undergoing ST&E to present the documentation needed to support test and populate their section of the Functional Description Document (FDD) prior to test commencement.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P36-4 The Company performs vendor screening of third party software development houses or providers prior to accepting software into the enterprise environment, with at least the following conditions required: 1. No contract shall be approved by Security without a relatively recent security audit report about the vendor, provided by the vendor, covering the service to be provided. 2. Audit reports for other service providers within the chain of service shall be reviewed on a case-by-case basis. 3. Data type, sensitivity and protection shall be principal considerations when screening the vendor. 4. Security shall provide a formal judgment of potential risks of vendors under consideration. This message supports the acquisition project or program in entering contracts with providers. P36-5 The Company uses ST&E to verify that potential threats and attendant enterprise risks associated with specific applications or systems have been neutralized or removed in code implementation. P36-6 The Company prioritizes testing and remediation tasks that align with enterprise risks and organizational strategies. P35-7 The Company provides resources in development projects that aim specifically to prevent the most likely and most harmful types of malfunction, intrusion, breach or attack, especially in those applications that process or transfer privacy-related data. P36-8 The Company structures its development and security testing processes to identify functional areas requiring additional emphasis, and then using this data to show progress toward organizational goals in software quality and security.	IT36-4 The Company tests APIs offered as part of cloud services and applications, evaluating authentication, access control, encryption methods, and activity monitoring as a minimum. IT36-5 The Company performs security-focused code review and penetration testing against applications that use external (third-party) APIs for access or interface to cloud applications. IT36-6 The Company conducts periodic ST&E re-test of all enterprise applications to check for mitigated security issues; changes in operational application circumstance or context; new sources of risk from threat intelligence; or potential interoperability problems from application portfolio expansion. IT36-7 The Company requires all applications or software products undergoing ST&E to present the documentation needed to support test and populate their section of the enterprise architecture and application portfolio documentation prior to test commencement. IT36-8 The Company conducts software ST&E on representative enterprise machines and systems to replicate expected loads, determine behaviors, and identify run-time services, protocols and ports required for the software or system to run correctly. IT36-9 The Company tracks all software projects, applications, systems or components which have ST&E discrepancies as a result of inherited enterprise issues, i.e., downstream or host system present vulnerabilities that affect the software under test, as IT Technical Debt to be addressed in governance and capital planning. IT36-10 The Company tracks all applications that are shown to contain security discrepancies during ST&E, ensuring that faults are corrected or mitigated, then re-tested prior to being deployed to operational systems. Discrepancies not resolved prior to deployment remain on the IT Technical Debt register until completion.	

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P36-9 The Company requires software to protect user credentials and prevent credential capture or theft. P36-10 The Company requires all software to enforce access controls, either mandatory or discretionary, in mechanisms that allow the enterprise to restrict and monitor data accessed by software users. P36-11 The Company tests all software test and development environments to confirm the test environment adequately reflects the expected operational environment for security controls and nonfunctional requirements.	IT36-11 The Company uses ST&E to verify proper safeguards are met when dispensation is given for software applications or systems to use insecure protocols as part of their engineering implementation.	
(37) Provide and Use Audit ***Best Practices Include*** *The Company uses audit procedures to understand internal compliance with enterprise direction and guidance.* *The Company uses audit procedures to understand enterprise technical agreement with external compliance regimes, to which the Company must comply and report.* *The Company uses audit reports to verify risk assessments and risk conditions.* *The Company's audit personnel protect information assets and watch for cybersecurity discrepancies or threats during audit events.*	***Process Specification Requirement*** P37-1 The Company defines and operates processes needed to meet policy requirements set forth for enterprise directives, instructions and guidance. P37-2 The Company understands and trains personnel to the requirements the enterprise must meet coming from applicable external laws, regulations, policy and guidance. P37-3 The Company implements either automated or manual processes that link technology system access with Human Resources to automate employee provisioning and deprovisioning to the greatest possible extent without introducing errors. P37-4 The Company uses periodic audit results to build a baseline of operations, and to indicate gaps or overlaps that are managed by governance and capital planning processes. P37-5 The Company uses periodic audit events – at least every twelve months – to verify existing enterprise risk conditions, to validate proposed mitigations and time schedules for discrepancy correction, and to find any unaccounted risk conditions that must be added to enterprise risk management.	***Information Technology Specification Requirements*** IT37-1 The Company maintains a compendium of IT policies and procedures, along with system topologies and operations diagrams, to enable auditors to understand the enterprise environment quickly. IT37-2 The Company maintains a set of automated tools for both endpoint examination and periodic sweeps that can be used by IT personnel as ongoing management or audit checks of the networks and enterprise systems. IT37-3 The Company conducts periodic audits of endpoint local storage (disk drives) with enterprise-owned tools to monitor for unauthorized software and/or unauthorized file storage. IT37-4 The Company grants access privileges to audit team personnel upon commencement of an audit work effort, but removes both access and technical means (2-factor authentication, enterprise equipment, etc.,) as soon as the audit is complete and when the audit team no longer has need to know.	***Operational Technology Specification Requirements*** OT37-1 The Company references the ICS-FDD software inventory for ICS evolution control, system maintenance, personnel training, supplier management, and periodic ICS internal and regulatory audits. OT37-2 The Company uses periodic tests and audits to confirm that no administrative functions from general-purpose networks (mail, etc.) are available on OT or process control systems or interface systems, appliances or devices. OT37-3 The Company performs periodic reviews of the ICS security incident detection policies and procedures to determine if those policies and procedures sufficiently enable employees and suppliers to protect marine or offshore ICS installation from risks described in the Risk Management process; the reviews provide an annual report to the ICS Security Office (if 3rd-party auditor performs audit) that documents the nature and number of gaps found, and recommends incident detection process and technology improvements, as well as policy and procedure updates.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	P37-6 The Company uses external audit reports for third party supplier or contractor verification, reinforcing the organizational due diligence processes and revealing any other conditions about third parties that may not be revealed in enterprise examinations. P37-7 The Company uses continuous audit and assessment of compliance requirements.	IT37-5 The Company conducts a walk-through with audit team personnel to confirm no residual equipment, systems or software from the audit and its tests are left behind at completion of the work effort. IT37-6 The Company uses audit techniques to verify configuration management program consistency and effectiveness throughout the enterprise. IT37-7 The Company uses audit techniques and tools to verify access authorization to critical systems is strictly accountable, universally logged, and granted or revoked in accordance with established and effective policies in the enterprise.	OT37-4 The Company conducts a walk-through of OT/ICS spaces with audit team personnel to confirm no residual equipment, systems or software from the audit and its tests are left behind at completion of the work effort.

SECTION 6 Cybersecurity Management System

1 Management of CyberSafety

A Company seeking to build or develop its cybersecurity program for certification under ABS CyberSafety™ is to implement and monitor its security strategy and plan through a Cybersecurity Management System (CMS), which is the capability management and tracking management framework designated for use in cross-security practices, programs and processes. *The CMS provides the management system nucleus for growing organizational capabilities to desired maturity levels; supporting operational understanding of security posture(s); satisfying audit requirements; and provisioning and maintaining security continuous monitoring (SCM) needs.*

Organizational Security personnel execute the CMS as the direct flow-down from the overarching enterprise technology and security strategies and any related implementation plans. The CMS provides prioritization and management of efforts to mature and complete the security architecture and the organizational capabilities required to meet enterprise security needs. It is to be demonstrated that the CMS objectives:

i) Maintain capabilities in the Company to understand and manage

- *a)* Systems and applications within the enterprise
- *b)* Data repositories and data stores serving enterprise applications and uses
- *c)* Data flows that support mission-critical applications
- *d)* Data flows that support mission performance measures
- *e)* Application performance measures and their indications applicable to security conditions
- *f)* Relationships among individual system security postures
- *g)* Overall networked system risk posture

ii) Develop, maintain and sustain an integrated risk profile for the enterprise

- *a)* Provide understanding of risk factors and possible risk impacts of threats, both external and internal, on overall mission, systems, data, organization, and facilities
- *b)* Prioritize risk mitigation and issue remediation work efforts based on threats, vulnerabilities and exposures of vulnerable systems or features to threats
- *c)* Certify system, unit, facility or organizational performance, and the ability to employ systems of systems for mission requirements
- *d)* Provide incident response capability for mission resilience in the expected threat environment, in consonance with risk postures

iii) Define sufficiency of protective measures and controls

- *a)* All perimeter and monitoring devices communicate with the enterprise log management or Security Information and Event Management (SIEM) system
- *b)* All security, perimeter and monitoring systems provide dashboard displays to support Security Continuous Monitoring (SCM)
- *c)* All communication paths go through security systems for monitoring and traffic filtering
- *d)* All web-based applications have web application protections (i.e., firewalling) in place
- *e)* All enterprise systems have host-based protections that report through monitoring dashboards

f) All security personnel understand monitoring measures and metrics, with ongoing training for continuity

g) All workstations and data stores have backups in protected, segregated storage

h) All enterprise personnel records and entities are part of the enterprise identity and access management regime;

i) All software is tested throughout its lifecycle for security integration

j) All enterprise systems are included in configuration, vulnerability and patch management processes

k) Configuration, vulnerability and patch management processes are informed by threat research and intelligence to provide prioritization feedback to risk management authorities

l) All enterprise systems are initially configured with, and managed through, system hardening guides in accordance with enterprise baseline and architectural controls

m) Enterprise systems are included in a security systems runbook

iv) Provide an integrated, interoperable security and perimeter device environment to enable

a) System automation, where advisable

b) Accelerated situational awareness and status understanding

c) Reduced staff requirements in data gathering

d) Shorter timelines for incident response, brought by quicker awareness

e) Improved daily system management, with greater supportability, reliability and maintainability

The CMS is the operational security management and reporting method which encourages completeness of effort, wholeness of security, and maturity of processes within the Company. Execution of CMS is to be applied across the entire Company. Proactive policies and protective controls are to be applied across the enterprise, modified to accommodate:

i) Physical locations for data and systems

a) Data center(s) and disaster recovery facilities

b) Physical facilities and document stores

c) Distributed digital data stores within facilities

d) Geo-limited data siloes with limited external accessibility

e) Endpoints and removable media

f) Physical storage locations for media and data

i) Mobile devices and storage

ii) Logical locations for data

a) Endpoints

b) Mobile devices

c) Shared drives

d) Segregated storage drives

e) Collaborative data stores

1) Line of business data stores

2) Collaborative environment data stores (e.g., SharePoint)

f) Backup data sets

g) Cloud services: applications (software as a service)

h) Cloud services: storage (infrastructure as a service)

i) Data archives

iii) Access rules for data and enterprise functions, as classified as

a) Roles

1) Employees

2) Contractors (on-site)

3) Consultants (on-site)

4) Contractors or consultants (off-site)

5) Retired employees

6) Customers

b) Rules

1) Project authorizations

2) Need-to-know

3) Minimum privilege

4) Separation of duties

c) Exceptions and special cases

1) Service accounts

2) Test accounts

3) Developer accounts, especially when geographically remote.

CMS management is per the CyberSafety capability level implementation plan. Capabilities are tracked and reported as necessary inside the Company.

Capability: CS1	*Personnel Assigned*	*Current Status/Exceptions for Reporting*
Exercise Best Practices		
Build the Security Organization		
Provision for Employee Awareness and Training		
Perform Risk Assessment		
Provide Perimeter Defense		
Prepare for Incident Response and Recovery		
Provide Physical Security		
Execute Access Management		
Confirm Asset Management		

Capability: CS2	*Personnel Assigned*	*Current Status/Exceptions for Reporting*
Perform Policy Management		
Provide Standards and Guidance		
Provide and Guide Cybersecurity Hygiene		
Gather and Use Threat Intelligence		
Perform Vulnerability Assessment		
Perform Risk Management		
Provide Data Protection		
Protect Operational Technology		
Perform System and Security Continuous Monitoring (SCM)		
Plan for Disaster Recovery (DR)		
Provide Unified Identity Management		
Perform System, Software and Application Test		
Perform System and Application Patch and Configuration Management		
Execute Change Control		

Capability: CS3	*Personnel Assigned*	*Current Status/Exceptions for Reporting*
Execute Capital Planning and Investment Control (CPIC)		
Implement Architecture Management		
Provide Secure Engineering		
Exercise Penetration Testing		
Build Forensic Analysis		
Enforce Privacy Data Management		
Provide Mobile Data Management (MDM)		
Provide Certificate Management		
Exercise Communications Management		
Enforce Network Access Control (NAC)		
Enforce Third Party Access Management		
Implement Secure Software Development		
Execute Security Test & Evaluation (ST&E)		
Provide and Use Audit		

3 Planning

3.1 Cybersecurity Environment Aspects

The Company is to establish, implement, and maintain procedure(s) to identify the contextual aspects of its shipboard and shore-based operations within the scope of the cybersecurity management system that it can control and those it can influence, taking into account planned or new developments or new or modified activities and services. The Company is to determine which aspects of its current circumstance have or can have a significant impact on the cybersecurity conditions in the Company. The Company is to document this information and keep it up-to-date in the Risk Management Plan and/or in the Security Functional Description Document (SFDD).

The Company is to take into account the significant contextual aspects when establishing, implementing, and maintaining its cybersecurity management system.

3.3 Cybersecurity Implementation Planning

The Company is to conduct and document a cybersecurity planning process. Cybersecurity planning shall be consistent with the Company's technology Acceptable Use Policy and shall lead to activities that continually improve performance. Cybersecurity planning is to involve a review of the Company's activities that can affect relative risk management performance.

3.5 Cybersecurity Hazard Identification, Risk Assessment, and Risk Control

3.5.1 Procedure(s)

The Company is to establish and maintain procedures for the ongoing cyber-physical system hazard identification, risk assessment, and determination of necessary controls. The procedure(s) for cyber-physical system or process hazard identification and risk assessment is to take into account:

i) Routine and non-routine activities involving the systems;

ii) Activities of all personnel having access to the workplace (employees, contractors, consultants, and including subcontractors, third party suppliers and visitors);

iii) Human behavior, capabilities, and other human factors in usability and potential effects of cyber-physical system malfunction;

iv) Hazards created in the vicinity of the workplace by work-related activities on or with cyber-physical systems under the control of the Company;

v) Cyber-enabled infrastructure, equipment, and materials at the workplace, whether provided by the Company or others;

vi) Changes or proposed changes in the Company, its activities, or materials;

vii) Modifications to the cybersecurity management system, including temporary changes, and their impacts on system operations, cyber-enabled system processes, risk management, and risk-related activities;

viii) Any applicable legal obligations relating to risk assessment and implementation of necessary controls that affect either personnel, the ship or asset, or the outside environment;

ix) The design of work areas, human work processes, cyber-physical system operations, system installations, machinery/equipment present, operating procedures, and work organization, including their adaptation to human capabilities (*Note:* modeled on OHSAS 18001:2007 4.3.1); and

x) Any potential environmental conditions that would affect existing cyber-enabled systems and procedures (e.g., environmentally-caused system failure), or CyberSafety-related conditions or procedures, such as if disaster event recovery efforts required all wireless network access points to be made open-access for recovery workers.

3.5.2 Methodology

The Company's methodology for cyber-physical system hazard identification and risk assessment is to:

i) Be defined with respect to its scope, nature, and timing to confirm it is proactive rather than reactive; and

ii) Provide for the identification, prioritization, and documentation of cyber-enabled system risks and the application of controls for either local and remote access or operation, as appropriate.

3.5.3 Management of Change

For the management of change, the Company is to identify the cybersecurity hazards and cyber-physical system operational risks associated with changes in the Company, the cybersecurity management system, or its activities, prior to the introduction of such changes.

3.5.4 Assessment Results

The Company is to confirm that the results of these assessments are considered when determining controls.

3.5.5 Cybersecurity Controls

When determining cybersecurity controls, or considering changes to existing cybersecurity controls, consideration shall be given to reducing understood or potential risks according to the following hierarchy:

i) Elimination

ii) Substitution

iii) Engineering controls or mitigation actions

iv) Signage/warnings and/or administrative controls

v) Personal protective equipment

vi) Transference of the risk, or sharing of the risk with other entities that may share supervisory or monitoring responsibilities with the Company

3.5.6 Functional Description Document

The Company shall document and keep the results of identification of hazards, risk assessments and determined controls up-to-date in the Risk Management Plan and/or in the Functional Description Document (FDD). Appendix 1 lists expected documents and artifacts to include within the FDD.

3.5.7 Cyber-physical System Risks and Controls

The Company is to confirm that the cyber-physical system risks and determined controls are taken into account when establishing, implementing, and maintaining its cybersecurity management system.

3.7 Legal and Other Requirements

3.7.1 Documented Procedure

The Company is to establish, implement, and maintain a documented procedure:

i) To identify mandatory rules and regulations applicable to both ship and shore-based operations;

ii) To identify applicable codes, guidelines, and standards recommended by the IMO, Administrations, classification societies, and maritime or control system industry organizations;

iii) For identifying and accessing the legal and other requirements to which the Company subscribes that are applicable to its cybersecurity compliance requirements; and

iv) For periodically evaluating compliance at least once every 12 months with applicable legal or regulatory requirements for cybersecurity, and other requirements to which the Company subscribes. The Company shall keep records of the results of the periodic evaluations in the Risk Management Plan and/or in the Functional Description Document (FDD).

3.7.2 Legal and Other Requirements

The Company is to take into account applicable legal requirements and other requirements to which the Company subscribes in establishing, implementing and maintaining its cybersecurity management system. The Company is to review the legal and other requirements at least once every 12 months and keep this information up-to-date in the Risk Management Plan and/or in the Functional Description Document (FDD).

3.9 CyberSafety Baseline

The Company is to establish a cybersecurity baseline using the information in the initial ABS CyberSafety™ review, considering the Company's cybersecurity posture and findings of the review. Changes in cybersecurity posture are to be measured against the cybersecurity baseline and tracked or managed in the cybersecurity management plan, or if appropriate, in the Risk Management Plan and/or in the Functional Description Document (FDD).

3.11 Management Programs

3.11.1 General

3.11.1(a) The Company is to establish, implement, and maintain programs for achieving its objectives and targets taking into account the unique design characteristics and operating requirements of each ship type, its cyber-enabled systems, its cyber-physical (control) systems, and their potential effects both onboard and offboard the ship or asset.

3.11.1(b) The Company shall determine the processes needed for the cybersecurity management system and their application throughout the Company. The Company is to determine the sequence and interaction of these processes.

3.11.1(c) The programs are to:

i) Identify criteria, methods, resources, and information required to effectively monitor, measure where applicable, analyze, control, and implement the identified processes in operating the cybersecurity management system, or its related safety or environmental impact control processes;

ii) Include defined levels of responsibility and authority and lines of communication between, and amongst, shore and shipboard personnel in expected aspects of cyber-enabled or cyber-physical system operations;

iii) Include the means, responsibility assignments and time frame by which the objectives and targets of the cybersecurity management system are to be achieved, including parameters to be monitored, and casualty control reaction procedures or processes identified and documented;

iv) Be reviewed at regular and planned intervals and updated as necessary, so that objectives are achieved.

3.11.1(d) These processes are to be managed by the Company in accordance with the requirements of this Guide.

3.11.1(e) Where the Company "chooses to outsource any process that affects product conformity to requirements, the Company shall confirm control over such processes. The type and extent of control to be applied to these outsourced processes shall be defined within the management system". (ISO 9001:2015, 4.1)

3.13 Cybersecurity Management System Documentation

The Company is to describe the pertinent cybersecurity-related security, health, safety, or environmental protection program effects or impacts, within the management system documentation, as applicable. Each and every cyber-physical system with potential impacts on health, safety or environment is to be documented.

3.13.1 Cyber-physical System Documentation

The cybersecurity management system documentation is to:

i) Define and document the scope of the cybersecurity management system including details and justification for any exclusions;

ii) Include pertinent Company policies, objectives and targets;

iii) Define the responsibility, authority, and interrelation of the personnel who manage, perform, and verify work relating to and affecting cyber-physical system security or cybersecurity, safety operations, or environmental effects, as appropriate;

iv) Describe the core elements and outline the structure of the Company's cybersecurity management system and interaction of its elements, and reference to related documents;

v) Include documented procedures established for the cybersecurity management system or provide appropriate references to cybersecurity management system documentation. The complexity of the work and the skill level of personnel involved in performing the work and the work environment shall govern the degree of control provided within management system procedures;

vi) Describe the interaction between the processes of the cybersecurity management system, indicating any dependencies or critical enabling factors that must be considered;

vii) Include the procedures and records required by this Guide to demonstrate conformity to CyberSafety capability level requirements and the effective planning, operation, and control of the cybersecurity management system processes.

viii) Include documents, including records, determined by the Company to be necessary to demonstrate the effective planning, operation, and control of processes that relate to its significant CyberSafety aspects and management of its cybersecurity risks to both IT and OT systems; and

ix) Be kept in the form that the Company considers most effective in the cybersecurity management plan, the Risk Management Plan and/or in the Functional Description Document (FDD).

5 Implementation and Operation

5.1 Resources, Roles, Responsibility, Accountability, and Authority

5.1.1 Resources

The Company's top management is to determine and provide the resources essential to establish, implement, maintain, and improve the cybersecurity management system. Resources include human resources and specialized skills, organizational infrastructure, technology, and financial resources. Resources also include personnel suitably trained to perform verification activities including internal management system or cybersecurity audits.

5.1.2 Roles and Responsibilities

The Company's management is to demonstrate its commitment by defining roles, allocating responsibilities and accountabilities, and delegating authorities, to facilitate effective cybersecurity management. Roles, responsibilities, accountabilities and authorities are to be defined, documented, and communicated. All those with management responsibility are to demonstrate their commitment to the continual improvement of cybersecurity performance. Top management it to take ultimate responsibility for cybersecurity and the cybersecurity management system.

5.3 Master's Responsibility and Authority

The Company is to clearly define and document the Master's responsibility with regard to: (Adapted from ISM 5.1)

i) Implementing the security controls designated for use with cyber-enabled and cyber-physical systems in accordance with policy of the Company;

ii) Motivating the crew to observe that policy;

iii) Issuing appropriate orders and instructions in a clear and simple manner;

iv) Verifying that specified requirements are observed; and

v) Periodically reviewing the cybersecurity management system and reporting its satisfactory performance or its deficiencies to the shore-based management.

The Company is to confirm that the cybersecurity management system operating on board the ship contains a clear statement emphasizing the Master's authority. The Company establishes in the cybersecurity management system that the Master has the overriding authority and the responsibility to make decisions with respect to personnel, system, ship or asset security, safety and pollution prevention, and to request the Company's assistance as may be necessary. (Adapted from ISM 5.2)

5.5 Shipboard Personnel

5.5.1 Master's Qualification and Support

The Company shall confirm that the Master is (Adapted from ISM 6.1):

i) Properly qualified for command;

ii) Fully conversant with Company's cybersecurity management system; and

iii) Given the necessary support so that the Master's duties can be effectively performed in ensuring the CyberSafety of the ship, its systems, and its cyber-physical functions.

5.5.2 Crew

i) The Company is to establish procedures to confirm that new personnel and personnel transferred to new assignments related to cyber-physical systems, their safety and security, and protection of cyber-enabled systems that could affect the environment, are given proper familiarization with their duties. Instructions which are essential to be provided prior to sailing should be identified, documented and given." (Adapted from ISM 6.3)

ii) The Company is to establish procedures by which the ship's personnel receive relevant information on the cybersecurity management system in a working language or languages understood by them. (Adapted from ISM 6.6)

iii) The Company is to confirm that the ship's personnel are able to communicate effectively in the execution of their duties related to the cybersecurity management system. (Adapted from ISM 6.7)

iv) The Company is to confirm that persons in the workplace take responsibility for aspects of cybersecurity over which they have control, including adherence to the Company's applicable cybersecurity requirements.

5.7 Control of Documents

5.7.1 Cybersecurity Management System Documentation

Cybersecurity Management System documentation consists of:

i) Established, implemented, and documented procedures for:

a) Policy and procedural document and data control, including documents of external origin;

b) Security or cybersecurity internal audits;

c) Security-related corrective and preventive action;

d) System non-conformances, declared incidents, hazardous occurrences and near misses;

e) Control of system testing and quality records;

ii) Documented system or application test (quality) policy and security testing objectives;

iii) A testing and system quality manual;

iv) Documents required for effective planning, operation and control of its processes; and

v) Records required to demonstrate compliance with requirements and of effective operation of the management system. (*Note:* The documentation can be in any form or type of medium.)

5.9 Operational Control

5.9.1 Shipboard Cyber-related Operations

The Company is to establish procedures, plans and instructions, including checklists as appropriate, for key shore-based and shipboard cyber-related operations and activities concerning the safety of personnel, safety of the ship, prevention of pollution, or other activities that can be affected by software-intensive or cyber-physical systems, in support of the Company policy(s), objectives, targets and action plans. The various tasks are to be defined and assigned to qualified personnel.

5.9.2 Flag State

The Company is to establish, implement, and maintain documented instructions and procedures to promote cyber-safe operation of ships, offshore assets and the associated shoreside facilities and protection of the environment in compliance with relevant international and Flag State legislation.

5.9.3 Controlled Conditions

The Company is to identify those operations and activities that are associated with identified hazards and significant cyber-enabled system risk areas where control measures need to be applied to manage the risk(s). Such controls include software management of change. The Company is to plan these operations and activities in order that they are carried out under controlled conditions. The output of this planning is to be in the form suitable for the Company's method of operations. Controlled conditions include:

i) Compliance with mandatory rules, regulations, and codes;

ii) Established and maintained documented procedures/work instructions to control situations where their absence could lead to deviation from the policies, objectives, and targets;

iii) Defined tasks assigned to properly qualified personnel;

iv) The Company's permit to work systems, which shall include measures to verify that the condition of spaces and systems as safe or not safe for work is readily identifiable. These measures shall also include safeguards so that work does not proceed unless safe conditions exist. The condition of spaces or systems being worked on shall be updated as appropriate throughout the course of the work;

v) Supply chain controls related to purchased goods, equipment, and services;

vi) Third party access controls related to contractors and other visitors to the workplace;

vii) The availability of suitable monitoring and measuring equipment;

viii) Implementation of monitoring and measurement; and

ix) Validation of approved processes and equipment, as appropriate, and required records

SECTION 7 Surveys After Construction and Maintenance of Class: ABS CyberSafety™ Requirements

1 General

The provisions of this Section are requirements for the maintenance of classification of the automated and cyber-enabled system(s) associated with the ABS CyberSafety™ (**CS**) notation. These requirements are in addition to the provisions noted in other ABS Rules and/or Guides, as applicable, to the vessel or facility.

For purposes of this Section, the commissioning date will be the date on which a Surveyor issues an Interim Class Certificate to the vessel or facility with the **CS** notation.

3 Surveys for the ABS CyberSafety™ Notation

3.1 Survey Intervals and Maintenance Manuals/Records

All Annual and Special Periodical Surveys associated with the **CS** notation are to be carried out at the same time and interval as the periodical classification survey of the vessel or facility in order that they are recorded with the same crediting date.

An Annual Survey of the automated and cyber-enabled system(s) associated with the **CS** notation is to be carried out by a Surveyor within three months either way of each annual anniversary date of the initial certification survey.

A Special Periodical Survey of the automated and cyber-enabled system(s) associated with the **CS** notation is to be carried out within five years of the initial certification survey and at five-year intervals thereafter. **CS** surveys may be offered for survey prior to the due date when so desired, in which case, the survey will be credited as of that date. A Special Periodical Survey at the five-year interval will take the place of the annual survey for that year.

Maintenance and calibration records are to be kept and made available for review by the attending Surveyor. The maintenance records will be reviewed to establish the scope and content of the required Annual and Special Periodical Surveys that are to be carried out by a Surveyor. During the service life of the software system components, maintenance records are to be updated on a continuing basis.

3.1.1 Special Conditions

The Owner is to inform ABS whenever major changes occur in any safety-critical or mission-critical software systems (i.e., IL3), including systems, components or modules modified or installed in the automated and cyber-enabled system(s) with **CS** notation. ABS may audit the vessel upon notification of an IL3 system modification or installation.

3.3 Annual Surveys

At each Annual Survey, the Surveyor is to perform an integrated software and hardware configuration audit to include verification of the following:

i) Check of asset records against Functional Description Document to verify accuracy of asset management efforts.

ii) Change control procedures include periodic audits to confirm that procedures are also being followed.

iii) Examination of Control Equipment Registry in FDD

iv) Examination of Software Registry in FDD

v) Review of all control system Hardware Registry entries

vi) Review records of virus and malicious software scans, and perimeter protective device logs of any events of specific interest.

vii) Review records of cyber-enabled system incidents and the attendant incident response efforts, including service restoration and post-event analyses.

3.3.1 Examination of Control Equipment Registry

i) Identify control equipment that has been changed since the last audit.

ii) Record each changed equipment item.

iii) List all software hosted on the changed equipment.

iv) Identify all documentation impacted by the change.

v) Record each documentation change.

vi) Note any changes identified that were not listed on the registry.

3.3.2 Examination of Software Registry

i) Identify all control software that has been changed since the last audit.

ii) Record each software item change.

iii) Inspect all software hosted on the changed equipment identified in step 7/3.3.1.

iv) Record software changes on changed equipment in the Software Registry.

v) Identify all documentation impacted by the changes.

vi) Record all changed documentation in the software registry.

vii) Note any software changes identified that were not listed on the registry.

3.3.3 Review of Integrated Control System's Hardware Registry

i) Assess how closely the software management of change (MOC) process is followed by interviewing relevant Owner/DCO and vendor crew as well as reviewing supporting documentation.

ii) Where possible, identify weaknesses and recommend improvements to the process.

3.5 Special Periodical Surveys

The Special Periodical Survey is to include all items listed under the Annual Survey to the satisfaction of the attending Surveyor. Additional attention may be required for new systems placed aboard the asset, for new system automated interfaces, or for new application access methods (remote or mobile) to critical applications or data onboard the asset. The intent of the Special Periodical Survey is to look across the asset's history since the previous Special Periodical Survey to develop an appreciation for what hardware, software or Company capability changes have occurred that may have invalidated assumptions associated with prior security conditions or risk profiles.

3.7 Facility Surveys

Companies that opt for a Facility Survey in addition to a ship or offshore asset certification will gain the addition '**+**' on their Notation in the ABS *Record* (i.e., **CS1/2/3+,** as appropriate). The Facility Survey process will entail full evaluation of the 5-step process shown in Section 3, Figure 2.

The intent of the Facility Survey is to address integrated systems that pass data or control critical functions between Facility and ship (or platform or other examined asset), including the Company's ability to provide capabilities for CyberSafety across the Facility, while specifically looking at interface devices, methods and systems. To this end, a Facility under examination requires a Functional Description Document (FDD) just as a ship or offshore asset requires.

At each Facility Survey, the Surveyor is to perform an integrated software and hardware configuration audit to include verification of the following:

i) Check of asset records against the Facility's Functional Description Document to verify accuracy of asset management efforts.

ii) Change control procedures include periodic audits to confirm that procedures are also being followed.

iii) Examination of interface control systems in FDD

iv) Examination of access control lists and access grant procedures for interface control systems and remote access systems as listed in FDD

v) Examination of Software Registry in FDD

vi) Review of all control system Hardware Registry entries

vii) Review records of virus and malicious software scans, and perimeter protective device logs of any events of specific interest.

viii) Review records of cyber-enabled system incidents and the attendant incident response efforts, including service restoration and post-event analyses.

3.7.1 Examination of Software Registry

i) Identify all control software that has been changed since the last audit.

ii) Record each software item change.

iii) Inspect all software hosted on the changed equipment identified in step 7/3.3.1.

iv) Record software changes on changed equipment in the Software Registry.

v) Identify all documentation impacted by the changes.

vi) Record all changed documentation in the software registry.

vii) Note any software changes identified that were not listed on the registry.

3.7.2 Review of Integrated Control System's Hardware Registry

i) Assess how closely the software management of change (MOC) process is followed by interviewing relevant Owner/DCO and vendor crew as well as reviewing supporting documentation.

ii) Where possible, identify weaknesses and recommend improvements to the process.

5 Modifications, Damage and Repairs

When it is intended to carry out any modifications to the automated and cyber-enabled system that affects the **CS** notation of the vessel or facility, the details of such modifications are to be submitted for approval and the work is to be carried out to the satisfaction of the Surveyor.

When an automated and cyber-enabled system that affects the **CS** notation of the vessel or facility has suffered any damage, which may affect classification, ABS is to be notified and the damage is to be assessed by a Surveyor.

Where an automated and cyber-enabled system suffers a premature or unexpected failure, and are subsequently repaired or replaced without Surveyor attendance, details of the failure, including the damaged parts where practicable, are to be retained onboard for examination by the Surveyor during the next scheduled survey/visit. If failures are deemed to be a result of inadequate or inappropriate maintenance, the maintenance manual is to be amended and resubmitted for approval.

SECTION 8 The CS-Ready Notation *(15 June 2018)*

1 General

The Shipbuilder Integrator (SBI) is to comply with the requirements in this Section in order for a vessel under construction to receive a **CS-Ready** notation. This Section also provides guidance for gathering and organizing System Providers (SP) engineering documentation needed by the Owner/Operator to complete requirements for the **CS1** Notation after delivery.

ABS verifies conformity to the requirements of this Section before awarding a **CS-Ready** notation The **CS-Ready** notation focuses on cyber security Operational Technology (OT) protections for vessels during construction and at delivery.

OT in this context includes the Owner-selected Industrial Control System (ICS) as well as associated cyber security protective functions installed during construction by the SBI and/or SPs.

3 General Cyber Security Responsibilities During Construction

The SBI is responsible for defining the boundaries of critical systems to be included within the scope of the **CS-Ready** notation. It is expected that the scope has been agreed upon with the Owner.

i) SBI Responsibilities:

a) Manage, aggregate, and update SP's functionality and technical documentation for the selected systems as the critical systems evolve throughout construction to delivery.

b) Develop a topology drawing or listing of the control system's network connection architecture for the ICS.

c) Provide a description of functionality for any cyber security protective functions installed by the SBI.

d) Monitor SP conformity to SBI's physical security policies and procedures during construction.

e) Monitor SP conformity to SBI's Software Management of Change policies and procedures during construction.

f) Document, maintain and update the ICS software registry during construction.

g) Document, maintain and update the ICS hardware registry during construction.

h) It is recommended that the SBI collaborate with the Owner to validate selections of the protected systems or equipment to be included in the **CS-Ready** notation.

ii) SBI is responsible to obtain from the SP:

a) Description of functionality documents for installed control system(s) that includes updates implemented as the system evolves from requirement development through final acceptance at delivery.

b) Cyber security updates for SP embedded cyber security functions implemented as the system evolves to final acceptance at delivery. For SBI or third-party installed cyber security related components, provide necessary documentation to support management and access monitoring by the Owner.

iii) ABS Responsibilities:

a) Review SBI's physical security policies and procedures and SBI's adherence to those policies and procedures.

b) Review SBI conformance to applicable Management of Change policies and procedures.

c) Review of documentation, see Subsection 8/7

d) Attend the SBI facility and vessel during construction and at delivery to survey the systems installation is in accordance with the SBI's description of functionality documentation.

5 Ship Builder Integrator Requirements

The following Section provides **CS-Ready** requirements related to software, hardware, and documentation that the SBI is to provide to the Owner/Operator at delivery to facilitate the Owner's effort to obtain a **CS** notation. The requirements listed are drawn from Section 5 of this Guide. The specific language of some requirements has been modified to accommodate the SBI's capabilities and responsibilities.

The naming and numbering conventions presented in the ABS CyberSafety™ Capability Matrix in Section 5 is shown in brackets [ ] in this Section for consistency.

5.1 SBI's Policies and Procedures

5.1.1 Physical Security Policies and Procedures

The SBI's physical security program accommodates the following:

i) Physical security is in place so that the SBI can effectively manage personnel onboard the asset. [PB7-1, ITB7-2, OTB7-2]

ii) Safeguarding of drawings, programs and data related to ICS designs and installation associated with the **CS-Ready** notation. [PB7-2, PB9-3]

5.1.2 SBI Software Management of Change (SMoC)

The SBI SMoC policies and procedures are to accommodate the following:

i) SPs are required to inform SBI prior to or shortly after, software updates in the form of release notes or updates to the functionality documentation. [PB9-4, OTB9-2]

7 Deliverables

7.1 Ship Builder Integrator Deliverable

7.1.1 Aggregated and Revision Controlled Industrial Control System-Functional Description Document (ICS-FDD)

i) The SBI is to collect and aggregate the SP-provided and the SBI-provided descriptions of functionality documentation into a consolidated Industrial Control System-Functional Description Document (ICS-FDD).

ii) The ICS-FDD is to be updated with release notices or replaced with a revised SP's functionality documentation during construction and commissioning until delivery of the asset.

iii) The ICS-FDD is to identify systems equipped for remote access (over satellite and internet).

7.1.2 Cyber Security Protective Equipment

The SBI is to compile a list of any SP(s) or SBI cyber security protective equipment, programs or other functions installed aboard the asset, if any. If no cyber security protective equipment is installed during construction or integration phases, or if protective software programs or other functions are not installed, the SBI is to state that none were installed.

7.1.3 Overall Topology Drawing

The SBI is to develop and provide to the Owner an overall topology drawing of the involved system(s), connected network(s) and connected system(s) [OT9-1, P5-10]. The topology drawing is to show:

i) All involved OT, and all OT-IT digital connections, in a schematic configuration. The SBI may include operationally-relevant IT systems installed as part of the overall architecture topology;

ii) Connection(s) to office network, internet or satellite communication system;

iii) Cyber security protective function(s) (equipment or program;

iv) Network protocol for connected equipment (*Note:* may be separately listed with reference on the topology drawing; and

v) Remote monitoring connections for any system represented in the topology drawing.

Note: The remote I/O modules should be shown as a single line regardless of the number of I/O connections and locations. Remote modules include connections for remote performance monitoring by OEMs.

7.1.4 Software and Hardware Registries

i) SBI is to provide to the Owner a software registry upon asset delivery that contains the following:

a) Software version number of each ICS component software program;

b) Firmware version number of each control system component, referenced to components on the topology diagram;

c) Version number of any cyber security software (e.g., firewalls, antivirus, etc.) installed by either the SP or the SBI;

d) Antimalware version numbers (e.g., program and virus definition) for protective software installed by either the SP or SBI; and

e) Version numbers of software running on any cyber security hardware or infrastructure devices (e.g., switches, routers) installed by either the SP or the SBI.

ii) SBI is to provide to the Owner a hardware registry upon asset delivery containing the following:

a) Equiment model of all components of the control system;

b) Serial number of processor, network or communications module, I/O modules and power supplies;

c) Model number of control system components;

d) Model numbers of cyber security protective hardware; and

e) Serial numbers of any cyber security hardware (switches, routers) installed by either the SP or the SBI.

7.1.5 SBI Installed Equipment Access Control

The SBI is to provide password protection or equivalent means of security for systems, workstations and devices. Passwords and, where necessary, other means of controlled access such as locks with key register shall be provided to the owner at delivery. [PB5-3]

7.1.6 SBI Blocking of Ports

i) The SBI is to block accessible OT ports, including both USB and RJ45 connection ports, and provide to the Owner the key(s) to unblocking of the ports, if any. [PB7-5]

Note: Accessible ports are those not located in normally locked rooms or within cabinets. Areas where accessible ports are typically located are the bridge, engine room, control room, etc.

ii) The SBI is to block accessible IT ports, both USB and RJ45, of integrated Human Machine Interface computers or other computers connected to OT networks and provide the Owner the key to unblock the ports, if any. [PB7-5]

iii) The port blocker may or may not require a key to install or remove the port blocker.

iv) The port blocker may be made from any material.

7.1.7 Cyber Security Functions

i) The SBI is to follow 8/7.3 for any cyber security function installed.

7.1.8 Other Deliverable Documents

i) Copy of ISO 9001 or other quality certificate

ii) Copy of ISO27001 certificate, if any

7.3 The SBI is Responsible to Deliver from the System Provider

7.3.1 Description of Functionality, as Part of the Delivered Ship (Product) Documentation, for the Control System and Cyber Security Functions Installed

The description of functionality is to contain the following:

i) Description of the functionality of the system, or system of systems;

ii) Ports, Protocols and Services (PPS) required for normal operations and enabled, noting and implementing others as disabled;

iii) IP Address and protocol of network or serial communication;

iv) Any SP or SBI installed cyber security protective functions;

v) Functional descriptions of installed cyber security protective functions;

vi) Ports, Protocol and Services enabled or disabled, noting disabled PPS; and

vii) IP Address and protocol of network or serial communications

7.3.2 SP's Cyber Security Protective Functions.

When cyber security protective functions (antivirus, firewalls, etc.) are provided, then the SP is to provide the following:

i) Model numbers of components of the cyber security protective hardware;

ii) Serial numbers of components of the cyber security protective hardware;

iii) Virus definition version number at FAT and prior to delivery; and

iv) Version numbers of software running on cyber security protective hardware.

7.3.3 Other Documents to be Provided

i) Safety analysis (*Note:* FMEA is acceptable, if applicable to the system.)

ii) Safety review, if no safety analysis (FMEA) was performed

iii) Model numbers of all components of the control system

iv) Serial numbers of control system components

v) Firmware version number of components of the control system

vi) Version number of software (programming) version number at FAT and just before delivery

vii) Topology drawing that represents the functions provided in functionality documentation and as installed when delivered to the Owner

viii) SP provided component password list, changed from defaults

9 Survey

9.1 Survey During Construction

The deliverables listed below will be verified to be on board the vessel by the attending Surveyor prior to delivery:

i) ICS-FDD (8/7.1.1)

ii) Cyber security protective equipment list (8/7.1.2)

iii) Topology drawing (8/7.1.3)

iv) Software and hardware registries (8/7.1.4)

v) SBI provided password list or means of security has been received by the Owner (8/7.1.5)

vi) OT and IT ports blocked (8/7.1.6)

9.3 Duration of Notation

The **CS-Ready** notation is valid until crediting of the first Annual Survey. The **CS-Ready** notation may be replaced by a **CS** notation if the Owner complies with the applicable requirements of this Guide. Software updates and cyber security protective functions are normally updated over time to maintain protection levels, knowledge of risks, and corporate knowledge of systems as documented in the functionality documentation. The Owner is to advise ABS of these updates and any other changes made following delivery at the time of application for the **CS** notation.

APPENDIX 1 Sample CyberSafety Management System Compliance (CMSC) Certificate

COMPANY NAME AND DIVISION/DEPARTMENT

COMPANY SHIP NAMES OR DESIGNATION

ATTN: [COMPANY CONTACT NAME]
[COMPANY DIVISION/DEPARTMENT ADDRESS]
Telephone: [COMPANY TELEPHONE NUMBER]
Email: [COMPANY CONTACT EMAIL ADDRESS]
Web: [COMPANY WEB ADDRESS]

Description:

This assessment is a representation by ABS of the degree of conformity to, and implementation of, the policies and procedures related to applicable sections of **ABS Guide for Cybersecurity Implementation for the Marine and Offshore Industries – ABS CyberSafety™ Volume 2.** The scope and limitations of this assessment are detailed on the pages attached to this CyberSafety Management System Compliance Certificate (CMSC).

This ABS CyberSafety Management System Compliance Certificate for cybersecurity implementation is awarded to [COMPANY NAME]-[COMPANY DIVISION] based on conformity with the quality standards set by ABS' *Cybersecurity Guide* for cybersecurity management implementation. This certificate confirms that [COMPANY NAME]-[COMPANY DIVISION] has demonstrated application of capabilities, quality standards, procedures, and policies in cybersecurity onboard [COMPANY SHIP OR ASSET] sufficient for the implementation of ABS CyberSafety™ Volume 2.

The following systems were reviewed in this assessment:

[system1]

[system2]

[system3]

Term of Validity:

This CyberSafety Management System Compliance Certificate [CERTIFICATE NUMBER], dated [CERTIFICATE EFFECTIVE DATE] remains valid until [CERTIFICATE EXPIRATION DATE] or until the Rules or specifications used in the assessment are revised (whichever occurs first).

This CMSC is intended for a company with assets associated with an ABS classed vessel, MODU or facility which is in existence or under contract for construction on the date of the ABS Rules or specifications used to assess the Product.

Configuration or use changes of the assets assessed under this CCC requires notification of ABS and potential reassessment of the assets and their networks and connections.

DRAFT

APPENDIX 2 Sample Certificate of Cyber Compliance (CCC) for the Company

COMPANY NAME AND DIVISION/DEPARTMENT

ATTN: [COMPANY CONTACT NAME]
[COMPANY DIVISION/DEPARTMENT ADDRESS]
Telephone: [COMPANY TELEPHONE NUMBER]
Email: [COMPANY CONTACT EMAIL ADDRESS]
Web: [COMPANY WEB ADDRESS]

Description:

This assessment is a representation by ABS of the degree of conformity to, and implementation of, the policies and procedures related to applicable sections of **ABS Guide for Cybersecurity Implementation for the Marine and Offshore Industries – ABS CyberSafety™ Volume 2.** The scope and limitations of this assessment are detailed on the pages attached to this Certificate of Cyber Compliance Certificate (CCC).

This ABS Certificate of Cyber Compliance Certificate for cybersecurity implementation is awarded to [COMPANY NAME]-[COMPANY DIVISION] based on conformity with the quality standards set by ABS' *Cybersecurity Guide* for cybersecurity management implementation. This certificate confirms that [COMPANY NAME]-[COMPANY DIVISION] has demonstrated application of capabilities, quality standards, procedures, and policies in cybersecurity sufficient for the implementation of ABS CyberSafety™ Volume 2.

Term of Validity:

This Certificate of Cyber Compliance [CERTIFICATE NUMBER], dated [CERTIFICATE EFFECTIVE DATE] remains valid until [CERTIFICATE EXPIRATION DATE] or until the Rules or specifications used in the assessment are revised (whichever occurs first).

This CCC is intended for a company with assets associated with an ABS classed vessel, MODU or facility which is in existence or under contract for construction on the date of the ABS Rules or specifications used to assess the Product.

Configuration or use changes of the assets assessed under this CCC requires notification of ABS and potential reassessment of the assets and their networks and connections.

DRAFT