GUIDE FOR

ABS CYBERSAFETY® FOR EQUIPMENT MANUFACTURERS

ABS CyberSafety® VOLUME 7

OCTOBER 2019

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

1701 City Plaza Drive
Spring, TX 77389 USA

Foreword

This Guide describes the requirements for equipment or a computer-based system to receive recognition for compliance as part of the ABS CyberSafety® program. The process which requires cybersecurity vulnerabilities to be identified by the OEM, can be applied to a digitally-enabled component or a complex system. The recognition can be either an ABS CyberSafety Product Design Assessment Certificate or a Design Review Letter with an ABS CyberSafety declaration.

Contributions to cyber risk can enter the supply chain at all levels. Those risk contributors can be inherited by downstream users of the maritime equipment from providers of products and services. While contributions to cyber risk are generally the result of non-malicious behaviors, the impacts of these risks late in the supply chain (i.e., the owner or operator) can be significant.

This Guide is primarily intended for use by suppliers of computer-based equipment installed in Operational Technology (OT) environments. It is secondarily intended for suppliers of computer-based equipment and associated digital infrastructure equipment that support OT environments. The guidance is provided for suppliers who are committed to (a) managing maritime cyber risk within their products; and, (b) communicating potential product-related risk information to point-of-use clients.

The suppliers benefit by demonstrating commitment to industry of cybersecurity resilient computer-based systems or components. The suppliers also can offer supplier developed or third party tested cyber protective equipment or software which functions satisfactorily within the confines of a real-time computer-based system to mitigate cybersecurity vulnerabilities.

The owner's cyber risk analysis benefits from the disclosure of vulnerabilities, allowing the owner to select and install cybersecurity protection. To lower the owner's cybersecurity risk, the owner may install protections outside the boundary of the computer-based systems to limit or monitor data and access to the entire system. The owner may install manufacturer recommended additive cybersecurity protective equipment within the boundary of the computer-based system to limit or monitor data and access to a component or components of the computer-based system. Benefits of highly integrated cyber-enabled systems are increased safety, emerging "smart" capabilities, and crew and machinery efficiency.

The effective date of this Guide is 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

ABS CYBERSAFETY® FOR EQUIPMENT MANUFACTURERS

ABS CyberSafety® VOLUME 7

CONTENTS

SECTION 1 General

1 Scope

This Guide describes the requirements for equipment or a computer-based system to receive recognition for compliance as part of the ABS CyberSafety program. This can apply to a digitally-enabled component or a complex system. The recognition can be either an ABS CyberSafety Product Design Assessment Certificate or a Design Review Letter with an ABS CyberSafety declaration.

The criteria contained in this Guide are meant to be applicable to equipment under control by a computer-based system that, in its entirety, is collectively known as a "computer-based system". Cybersecurity vulnerabilities may be introduced into computer-based systems with some digital components, network architecture, system design, and software making up the computer-based system. Cybersecurity vulnerabilities become cybersecurity risks when they are accessed by persons or computers via digital endpoints. The owner risks from these vulnerabilities are mitigated by installing protective functions, or by using hardened configurations, controlled settings, and continuously monitoring the systems. This Guide is applicable to systems under control by one or more computer-based system(s) such as Power Management, Dynamic Positioning, Engine Control, etc.

A cybersecurity vulnerability is a condition that may allow a digital device or software application to be accessed by an unauthorized digital identity or human, resulting in potential digital corruption or functionality effects in the system or network. A vulnerability can exist in the equipment making up the computer-based system, third-party equipment connected to the computer-based system, and software and firmware executing on the components. These vulnerabilities can be eliminated with firmware or software updates, configuration changes, privilege changes, or architectural modifications. When found early in asset construction and system installation, integrators, shipyards, and owner/operators can manage related risks and/or embedded risk management solutions more efficiently and economically.

An ABS CyberSafety Product Design Assessment for a digitally-enabled component or complex system documents known cybersecurity vulnerabilities to facilitate an asset owner's cybersecurity risk analysis and remediation. The Original Equipment Manufacturer's (OEM) product receives an ABS CyberSafety Product Design Assessment Certificate or a Design Review Letter when it meets the requirements set forth in this publication.

The equipment may have cybersecurity vulnerabilities that may be mitigated by installing tested architecture equipment (routers, data diodes, etc.) or software (firewalls). Vulnerabilities also can be eliminated with software patches or updates. By understanding the unresolved vulnerabilities, the owner can choose to install hardware or other protective functions, modify architectures, or change processes to lessen the known vulnerability, and thus mitigate the owner's associated cybersecurity risk.

Computer-based systems that control production or operational systems, called Operational Technology (OT), are cyber-physical systems that control processes and systems. These OT systems have relevance to safety in their environments because they control the physical behaviors of connected equipment. They generally communicate with Information Technology (IT) general-purpose networks to provide sensed operational data to management personnel. Computer-based systems extend to the connected network and the components, as well as any IT equipment used to display data and for operator control.

Computer-based systems may be composed of the OEM's and sub-supplier's computer-based systems, computers, servers, or cyber-enabled and networking infrastructure components. Digitally-enabled Commercial-Off-The-Shelf (COTS) components may be installed in the computer-based system as well.

3 OEM Company Level Requirements

The development environment influences the component selection and programming of the computer-based system. Also, the environment is controlled by the OEM's policies and procedures, product change management, cybersecurity training, risk management, and other management processes to govern the product development and evolution. Because of the impact these documented processes have upon product development and evolution, ABS is to review these processes (See Section 1, Table 1).

The OEM has the greatest insight into their product as they can monitor their supply chain, select components, document cybersecurity vulnerabilities, and install or recommend cybersecurity protections if cybersecurity vulnerabilities are found within a component or computer-based system.

The OEM is able to verify if a component is listed in the NIST National Vulnerability Database or the OEM can purchase components that are cybersecurity certified with all other considerations being met. The OEM is to declare any cybersecurity vulnerabilities to downstream users. The integrator, shipyard and owner may then review the declared vulnerabilities of the computer-based system and determine cybersecurity protective equipment to install at the boundary of the computer-based system to mitigate the risk. It is recommended that, when installing cybersecurity protective equipment within the boundary of the real-time computer-based system, the OEM is involved, because potential data and command latency caused by cybersecurity protective equipment may affect system safety and performance.

Computer-based systems are relevant to safety in their environments since the equipment operates in real-time, and thus time delays in commands and data potentially caused by cybersecurity protective equipment are a concern. It is recommended that the OEM test cybersecurity protective equipment that functions within acceptable parameters for downstream integrators, shipyards and owners to install within the boundary of the computer-based system to mitigate any declared vulnerabilities.

The functional description, equipment list, topology drawing, and accessible connections of the computer-based system are addressed in this Guide as connections allow digital devices and human access to vulnerabilities. The remote connections and wireless networks are addressed with potential vulnerabilities (rogue wireless connections and Internet attacks on remote connections) and controls the OEM puts in place to mitigate access to wireless devices and access points and remote connections.

The component or computer-based system is to be programmed, developed, tested, and maintained in a cybersecure-controlled environment to minimize the introduction of cybersecurity vulnerabilities during these activities. The OEM may elect to be a certified Service Provider for ABS CyberSafety where ABS will review documents for compliance as listed in Section 1, Table 1.

TABLE 1
OEM Company Level Requirements

	Certified Service Provider (valid for 5 years)	*Not Certified as Service Provider*
Requirements:		Subsection 2/5
• Cyber Security Office	2/3.3.2	
• Incident Response Team	2/3.3.3	
• Cybersecurity Policies & Procedures	2/3.3.4	
• Internal Risk Management	2/3.3.5	
• Cybersecurity Training	2/3.3.6	
• Product Change Management	2/3.3.7	
• ABS Audit	4/3.1	No audit
Required For:	Computer-based system components requesting PDA or DRL approval and installed in: • Essential Services or safety systems • Category II or III Systems (see 2/1.1)	

TABLE 1 (continued)
OEM Company Level Requirements

	Certified Service Provider (valid for 5 years)	*Not Certified as Service Provider*
Suitable For:	• Complex functionality (as defined by OEM) • Frequent updates (OEM request a PDA revision for updates to the associated equipment PDAs) • Frequent customization • Large number of components requiring ABS approval	• Less complex functionality (as defined by OEM) • Infrequent updates • Limited customization • Smaller number of components seeking ABS approval • Network infrastructure components, printers, computer-based system components not installed in essential services • IOT or IIOT
Eligible for:	ABS CyberSafety Product Design Assessment or Design Review Letter with ABS CyberSafety declaration (DRL)	

5 Equipment Level Requirements

The OEM may request either an ABS CyberSafety Product Design Assessment (PDA) or a Design Review Letter with an ABS CyberSafety declaration. Both require a review of the OEM's computer-based system or component documentation that are listed in Section 1, Table 2.

TABLE 2
Equipment Level Requirements

	ABS CyberSafety PDA	*Design Review Letter with ABS CyberSafety Declaration (DRL)*
Applicability and Limitations:	Applicable to many applications with Service Restrictions listed on ABS CyberSafety PDA Certificate, valid for two (2) years	Restricted to specified equipment and vessels listed on DRL

Requirements:
Note: In addition to this Guide for the ABS CyberSafety PDA, the computer-based system or component is subject to Appendix 1-1-A3 of the ABS R*ules for Conditions of Classification (Part 1)* for the equipment PDA and the applicable Rules or Guide selected for a DRL. The equipment PDA is valid for 5-years.
	Vulnerability Report consisting of:
	• Vulnerability Analysis
	  ○ Known vulnerabilities
	  ○ Local and remote access management
	  ○ Wireless vulnerabilities and OEM installed controls
	  ○ Remote connection vulnerabilities and OEM installed controls
	  ○ Cybersecurity protective controls OEM installed or recommended
	  ○ Sub-supplier documents
	• Functionality of component or system
	• Controlled Equipment List
	• Topology drawing
		Vulnerability Report consisting of:
		• Vulnerability Analysis
		  ○ Known vulnerabilities
		  ○ Local and remote access management
		  ○ Wireless vulnerabilities and OEM installed controls
		  ○ Remote connection vulnerabilities and OEM installed controls
		  ○ Cybersecurity protective controls OEM installed or recommended
		  ○ Sub-supplier documents
		• Functionality of component or system
		• Controlled Equipment List
		• Topology drawing

	ABS CyberSafety PDA	*Design Review Letter with ABS CyberSafety Declaration (DRL)*
ABS CyberSafety Type Test:	See Subsection 4/1 for the CyberSafety Type Test *Note:* There may also be Type Testing required per Appendix 1-1-A3 of the ABS *Rules for Conditions of Classification (Part 1)* for the equipment PDA.	No ABS CyberSafety Type Test required

7 Limitations

i) ABS CyberSafety for Equipment Manufacturers is applicable to computer-based equipment, local and remote Human Machine Interfaces (HMI), and supporting IT systems connected to the computer-based equipment system(s) or network(s) in functional supporting roles. This includes the operating system, control system(s), and computers residing on the computer-based equipment network(s) and special-function IT systems that may affect performance of the computer-based system being approved. The programmed OT functionality of the system is not included in this Guide. Therefore, the programmed actions or purpose of the computer-based system is not reviewed or included as part of the ABS CyberSafety PDA or the Design Review Letter with ABS CyberSafety declaration.

ii) Modifications and actions by others affecting the computer-based system or its Cybersecurity Protective Functions (CSPF) applicable to the as-described and assessed computer-based system or component, when applied by any party, other than the OEM or submitter, including the owner, are not covered by the ABS CyberSafety PDA or Design Review Letter with ABS CyberSafety declaration. Only the as-delivered computer-based system and the as-described components and cybersecurity performance to either the integrator, shipyard, or owner is covered by the ABS CyberSafety PDA or Design Review Letter with ABS CyberSafety declaration. Additions to or modifications of the computer-based system and/or its associated network(s) by any other party to the computer-based system, OT or IT networks are not covered.

iii) The ABS CyberSafety PDA is based upon the OEM's documentation listing disclosed vulnerabilities and OEM cybersecurity described performance.

9 Definitions, Abbreviations, and References

9.1 Definitions

Accessible Physical Ports. Ports (such as RJ45, USB, etc.) that are not physically protected by cabinets (lockable or not), controlled spaces, or normally monitored or locked rooms.

Commercial-Off-The-Shelf (COTS). Denotes a component provided by a commercial supplier that is used as is, adapted, or configured for use, but not programmed specifically for the OEM's project.

Complex Connection. A digital communications path between equipment and a network that supports other digital communications but is not connected to the Internet.

Computer-based System. The equipment or system subject to the ABS CyberSafety PDA or DRL. A computer-based system performs a specified function, is commonly composed of electromechanical equipment connected to a single computer-based system or multiple computer-based systems, is a subset of Operational Technology (OT), and is usually a cyber-physical system controlling physical equipment in real time processing. The computer-based system's functionality is programmed for various conditions and the functionality is called OT Functionality.

Cybersecurity Protective Function (CSPF). Functions or controls that provides either physical (routers, programmed switches) or logical (software, i.e., firewalls) cybersecurity protection to mitigate a vulnerability.

Discrete Connection. A digital communications path characterized by one direct connection (not networked) to one piece of equipment, but not to the Internet.

Essential Services (Primary and Secondary). Services considered necessary for continuous operation to maintain propulsion and steering (primary essential services), non-continuous operation to maintain propulsion and steering and a minimum level of safety for the vessel's navigation and systems including safety for dangerous cargoes to be carried (secondary essential services), and emergency services as described in 4-8-1/7.3.3 of the ABS *Rules for Building and Classing Marine Vessels (Marine Vessel Rules)* (each service is either primary essential or secondary essential depending upon its nature). Also refer to essential services in 4-1-1/1.1.2, 4-1-1/3.5 and 4-1-1/Tables 3 and 4 of the ABS *Rules for Building and Classing Mobile Offshore Units (MOU Rules)*.

Factory Acceptance Test (FAT). Testing of the computer-based system generally focused on testing the OT functionality, usually at the manufacturer's facilities.

Integrity Level. Used here it is an OEM-assigned value from 0 to 3 of the severity of computer-based system failure defined in the ABS *Guide for Integrated System Quality Management (ISQM Guide)* based upon safety, environment, and asset's mission considerations. See Section 3, Table 1 of the *ISQM Guide*.

Media Access Control (MAC). Address for Ethernet hardware address assigned by the manufacturer of network cards and other layer 2 devices (switches, etc.) of the OSI model.

Node. A digital communications connection point capable of transmitting, receiving, or creating information over a communication channel. The node can use serial, network, and various protocols for passing digital information.

Original Equipment Manufacturer (OEM). A supplier that is the primary provider of a computer-based system.

Operational Technology (OT). Automated systems (cyber-physical), including hardware and software, that perform direct monitoring and/or control of physical devices, processes, or events. It is a superset of computer-based industrial control systems that includes monitoring, sensing, and human interface devices, as applicable to an installation.

OT Functionality. The programmed actions and purpose of the computer-based system and how the collective system is programmed during normal, degraded, and failed states or conditions.

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) (see the ABS *Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafety® Volume 2*).

Service Provider (SP). Voluntary certification for qualified service providers who offer specialized services and enhance existing marine and offshore safety practices offered by ABS. (https://www.eagle.org)

Simple Connection. A direct digital communications path between one piece of equipment and one or more other pieces of equipment (not networked), but not to the Internet.

Sub-supplier. A company providing digitally-enabled hardware that is programmed to meet the OEM's requirement(s) with a sub-system or programmed component. Excludes COTS and sub-suppliers who provide services or training on behalf of the OEM.

Sub-system. A programmed digitally-enabled set of components supplied to an OEM as a sub-component of the OEM's computer-based system as a custom-made solution. It excludes instrumentation, electrical breakers, Commercial-Off-The-Shelf (COTS) components connected to a wireless or wired network, and mechanical equipment (steel, bolts, concrete, etc.).

Very Large Network. A direct digital communication path between cyber-enabled equipment or network(s) to a node or endpoint accessible to a very large number of digital identities, such as the Internet.

Vulnerability. Used here, a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Source: NIST SP 800-53. It is a weakness that allows a digital device, endpoint, or software application to be accessed by an unauthorized digital or human identity and digitally corrupts or affects the functionality of the system or network.

9.3 Abbreviations

COTS	*C*ommercial-Off-The-Shelf products
CSO	Cyber Security Office
CSPF	Cybersecurity Protective Function(s)
CVSS	NIST NVD Common Vulnerability Scoring System (CVSS)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DRL	ABS Design Review Letter with ABS CyberSafety declaration
FAT	Factory Acceptance Test
HMI	Human Machine Interface
IIOT	Industrial Internet Of Things
IL	Integrity Level from Section 3, Table 1 of the *ISQM Guide*
IOT	Internet Of Things
IRT	Incident Response Team
ISQM	Integrated Software Quality Management
IT	Information Technology
MAC	Media Access Control
NIST	National Institute of Standards and Technology
NIST NVD	National Institute of Standards and Technology, National Vulnerabilities Database (https://nvd.nist.gov/)
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection
OT	Operational Technology
PDA	ABS Product Design Assessment Certificate
PPS	Ports Protocols and Services

9.5 Recognized Industry Standards

ABS *Guide for Cybersecurity Implementation for Marine and Offshore Operations – ABS CyberSafety® Volume 2*

ISA/IEC 62443-1 through 4 *Industrial Network and System Security*

ISO 27001 Security techniques – *Information security management systems – Requirements*

ISO 27002 Security techniques – *Code of practice for information security controls*

NIST CSF *Framework for Improving Critical Infrastructure Cybersecurity*

NIST SP 800-82 *Special Publication – Guide to Industrial Control Systems (ICS) Security, Revision 2*

NIST SP 800-53 *Special Publication – Recommended Security Controls for Federal Information Systems and Organizations*

9.7 References

ABS *Rules for Conditions of Classification (Part 1)*

ABS *Rules for Building and Classing Marine Vessels*

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

ABS *Guide for Integrated Software Quality Management*

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

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

ABS *Guide for Smart Functions for Marine Vessels and Offshore Units*

Cybersecurity Capability Maturity Model (C2M2), Office of Cybersecurity, Energy Security, and Emergency Response, US Department of Energy

SECTION 2 OEM Company Level Requirements

1 General

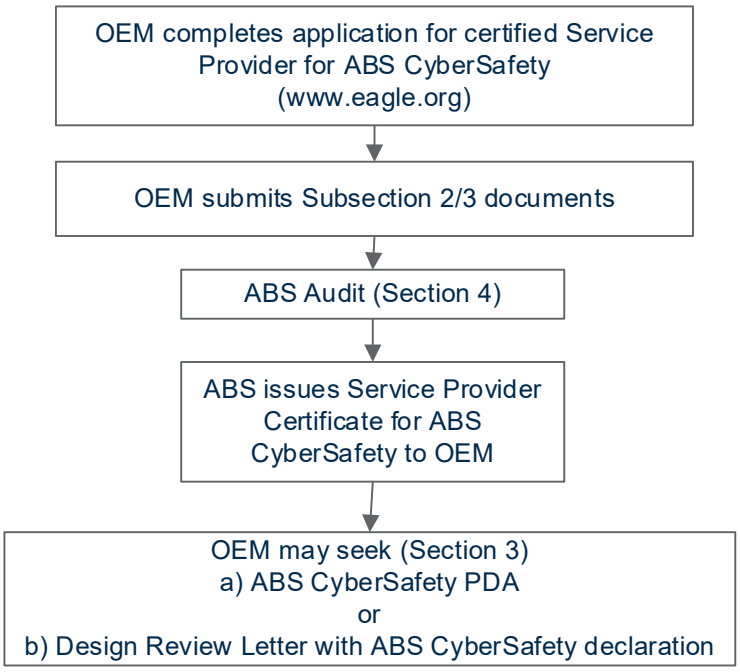
Products, components, and computer-based systems are to be developed in a cybersecure environment. In addition, ABS is to review the OEM's internal policies, procedures and cybersecurity processes, risk management and change management compared to the OEM's declared foundational standard.

The ABS CyberSafety PDA and DRL with ABS CyberSafety declaration is provided based on a review of OEM documentation for compliance with pertinent Rules or Guides and this Guide.

1.1 OEMs Who Desire to Become a Certified Service Provider for ABS CyberSafety

The OEM submits a Service Provider application noting ABS CyberSafety on the application. The OEM is to submit documents listed in Subsection 2/3. Upon meeting the requirements and passing the audit, ABS will issue a Service Provider Certificate for ABS CyberSafety to the OEM. Section 2, Figure 1 shows the process to receive a Service Provider Certificate for ABS CyberSafety.

FIGURE 1
Certified Service Provider Process



Recognition as a certified Service Provider is required for:

i) Computer-based system components installed in primary and secondary essential services (1/9.1) or safety systems delivered with an ABS CyberSafety PDA.

ii) Computer-based system components installed in primary and secondary essential services (1/9.1) or safety systems delivered with a Design Review Letter with ABS CyberSafety declaration.

iii) Computer-based system components installed within systems listed in System Categories II and III as defined in 4-9-3/Table 1 and Appendix 4-9-3A2 of the *Marine Vessel Rules* delivered with an ABS Cybersafety PDA.

iv) Computer-based system components installed within systems listed in System Categories II and III as defined in 4-9-3/Table 1 and Appendix 4-9-3A2 of the *Marine Vessel Rules* delivered with a Design Review Letter with ABS CyberSafety declaration.

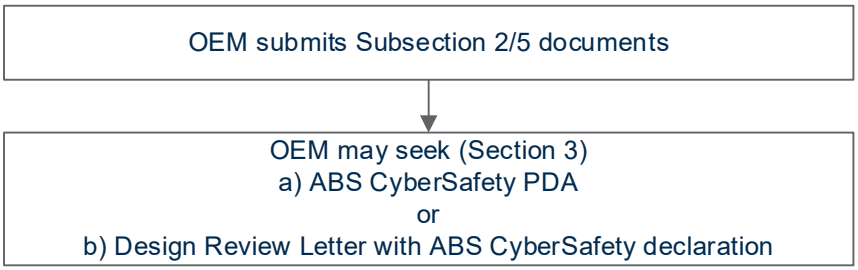
v) If the OEM's Service Provider Certificate is invalidated, for any reason, the ABS CyberSafety PDAs associated with systems listed in 2/1.1i) through iv) will be suspended until the Service Provider Certificate is revalidated.

The certified Service Provider for ABS CyberSafety is valid for five years and subject to annual audits. The OEM can apply for new ABS CyberSafety PDAs and DRLs for computer-based systems or components with existing equipment PDA or apply for new equipment PDAs with associated ABS CyberSafety PDAs while holding a valid ABS Service Provider Certificate for ABS CyberSafety.

1.3 Other than a Certified Service Provider

The OEM is to contact ABS to begin the review the OEM's internal cybersecurity policies, procedures, risk management and other cybersecurity controls. The OEM is to submit documents listed in Subsection 2/5 for the review submittals. Section 2, Figure 2 shows the process for the other than certified Service Provider.

FIGURE 2
Other than Certified Service Provider Process



3 OEM Certified Service Provider

3.1 Locations where OEM Software is Developed

The OEM is to submit documents for all locations where control system software is developed, tested, and maintained for the computer-based system(s) or components under consideration for an ABS CyberSafety PDAs or DRLs.

3.3 OEM Cybersecurity Documents to be Submitted for Review

OEM's revision-controlled documents which address the following are to be submitted:

3.3.1 OEM's Preferred Cybersecurity Standard

The OEM is to state the foundational standard or combination of standards used in development of their cybersecurity methodology. See 1/9.5.

3.3.2 OEM's Internal Cyber Security Office (CSO)

The OEM is to identify a person, organization, or office responsible for the internal IT and OT cybersecurity of the OEM's facilities in which product development is performed, as well as denote cybersecurity protections embedded in the product, as applicable. The OEM is to submit CSO documentation listed below:

i) Mission statement of the CSO with defined cybersecurity goals for computer-based systems

ii) Names or titles of the CSO members

iii) Roles and responsibilities of CSO members, including approvals and authorities

iv) OEM's organizational chart showing the CSO

The following are to be available to ABS upon request:

v) CSO audits or reviews

vi) Corporate technical risk tolerance and technical risk evaluation documentation

3.3.3 OEM's Incident Response Team Organization (IRT)

For the computer-based system under consideration for the ABS CyberSafety PDA or DRL:

i) The OEM is to have an organization, office or person(s) who are responsible for providing support to clients who require assistance recovering from a cyber-related software failure.

ii) The OEM is to have an Incident Response Plan with a recovery procedure

Note: The OEM is required to notify ABS per the agreed Terms and Conditions of the issued PDA.

iii) The OEM is to submit:

a) Incident Response Policy and Procedure

b) Mission statement of the IRT

c) Roles and responsibilities of team members, including approvals and authority

iv) The following are to be available to ABS upon request:

a) Incident Response Plan including the recovery procedure for the computer-based system [2/3.3.3ii)].

b) Indications of periodic performance of tabletop exercises focused on client recovery from a cyber incident.

c) Findings of any incident response investigation of a reported computer-based system failure, with approved remedies and implementation timeline, or the procedure for such investigation.

3.3.4 OEM's Cybersecurity Policies and Procedures

The OEM is to submit:

i) General Cybersecurity Policies and Procedures addressing:

a) Physical and access security

b) Acceptable use of OEM's digital devices including portable devices

c) Digital access, registration, and de-registration of OEM's personnel and contractors

1) Role-based least functionality assigned and limitation

2) Account management

3) Access control to OEM's IT and OT resources

4) Login identification and authentication

d) Protection of information (during processing, storage, and data breach response)

ii) Network Security Policies and Procedures

a) Remote access (into OEM's network)

b) Use of wireless and mobile devices at the client's site

3.3.5 OEM's Internal Risk Management

The OEM is to make available to ABS, upon request:

i) Enterprise and product cyber risk assessment policies and procedures.

ii) Documents describing periodic cyber risk assessment of enterprise business systems with consideration of controls in place to manage identified risks.

iii) Documents describing periodic technical cyber risk assessments of products, including risks identified, risks tolerated or accepted, controls embedded in products to manage identified risks, and controls recommended for managing risks after product implementation.

If the OEM has a current ISO 27001 Certificate, items 2/3.3.5i) and 2/3.3.5ii) are not required.

3.3.6 Cybersecurity Training

The OEM is to conduct periodic cybersecurity training of office and field personnel.

i) The OEM is to submit:

a) Cybersecurity awareness and training policy

b) The titles of provided training topics and titles of personnel who periodically receive the training. The training is to address:

1) Cyber hygiene (employees and contractors)

2) Use of portable digital devices (e.g., phone, memory devices, portable hard drives)

3) Security of company and client data

c) Records or logs of completions of training by personnel and contractors

d) On-boarding training topics for new personnel (if different from above)

e) Schedules of periodic refresher cybersecurity and change management policies and procedures training

3.3.7 OEM Change Management and Configuration Control

The OEM documents and implements change control procedures for internal enterprise business systems, product hardware, embedded software, and embedded cybersecurity controls, and production, testing, installation, and maintenance processes. The procedures are to define major and minor revisions, as well as extensive updates or significant modifications. The OEM is to denote:

i) Change management policy and/or procedure for hardware and software of computer-based systems

ii) Documentation indicating tracking of change management from request through implementation, upon request by ABS. The documentation is to detail:

a) Approval flow

b) Change document tracking

c) Internal testing

d) Implementation on client's platforms

iii) Description of software change management program or practices to manage inherent evolutionary conditions, denoting:

a) Changes to fielded control system requirements

b) Revisions to and updates in fielded control system applications

c) Fielded software incompatible with recommended or critical security updates

d) Low-impact replacement of fielded but unsupported control system software version(s)

3.3.8 Third Party Involvement in Programming of the OEM's Software

If a third party is involved from a remote location in the programming or software maintenance for the computer-based system being considered for an ABS CyberSafety PDA or DRL, then that company or companies are to be involved and provide required documents as listed in 2/3.3.1 through 2/3.3.7.

i) If the third party uses the same policy and procedures as the OEM, the third party is to state that they use the same policies and procedures as the OEM.

ii) If the third party uses different policy and procedures, the OEM is to submit documents listed (2/3.3.1 through 2/3.3.7) for the third party.

iii) The OEM is to provide a document detailing how the OEM receives, verifies, and tests software obtained from third parties.

3.5 Copies of Certificates

If the OEM holds any of the following certificates, copies are to be submitted.

i) ISO 9001 or equivalent

ii) ISO/IEC 27001

iii) ISA/IEC 62443

iv) ISASecure® Certificates (IEC 62443 conformance certificate)

In addition, any other cybersecurity certificates are to be noted and submitted.

3.7 ABS Certified Service Provider Initial Audit

After the OEM has closed all technical comments from the ABS engineering review, the OEM is to contact the local ABS Survey office for the audit. The audit requirements are listed in Subsection 4/3.

3.9 ABS Certified Service Provider

Upon the OEM meeting the requirements of 2/3.3 and the audit, the OEM is to receive the ABS Service Provider Certificate for ABS CyberSafety, and may proceed with the equipment document review (Section 3). The OEM is to complete a "Request for Certification – ABS Type Approval Product Design Assessment (PDA)" application (www.eagle.org) for the computer-based system or component to be design assessed. The computer-based system or component is to meet the requirements of the *Marine Vessel Rules* as well as the requirements listed in Section 3 of this Guide.

5 OEMs Other than ABS Certified Service Provider

5.1 Documents to be Submitted for Organization Cybersecurity Review

Documentation indicating the following are to be submitted:

i) The OEM's foundational cybersecurity guidance [2/3.3.1]

ii) The name of a person, organization or office responsible for cybersecurity of the enterprise and products.

iii) The composition and responsibilities of the cybersecurity Incident Response Team.

iv) OEM Cybersecurity Policies and Procedures detailing: [2/3.3.4]

a) Training in cyber hygiene and specialized cybersecurity functions

b) Physical access security [2/3.3.4i)a)]

c) Digital access, registration and de-registration of OEM's personnel and contractors [2/3.3.4i)c)]

d) Acceptable Use Policy for OEM's digital devices and portable devices [2/3.3.4i)b)]

v) Internal review of the technical cybersecurity risk inherent to the OEM's products.

vi) Documents indicating control of product change and configuration.

If the OEM holds cybersecurity and/or quality certificates listed in 2/3.5, copies are to be submitted.

SECTION 3 Equipment Level Requirements

1 General

Component selection, overall system design, architecture, and software may inadvertently introduce cybersecurity vulnerabilities that can be mitigated by appropriate cybersecurity controls. Equipment can be reviewed for either a Product Design Assessment or a Design Review Letter.

1.1 Design Review Letter with ABS CyberSafety Declaration (DRL)

The OEM is to contact ABS.

1.3 ABS CyberSafety PDA

The OEM is to submit a "Request for Certification – ABS Type Approval Product Design Assessment (PDA)" application (www.eagle.org) for the computer-based system or component to be design assessed.

1.5 Amending or New Product Design Assessment (PDA) or Type Approval

i) If the equipment, which includes the computer-based system, has a valid PDA or Type Approval Certificate, then:

a) The ABS CyberSafety application is to list the associated equipment PDAs or Type Approval number(s) and system identifier(s) to which the OEM is applying this ABS CyberSafety PDA Certificate.

ii) If the equipment, which includes the computer-based system, does not have a PDA and is not Type Approved, then:

a) The first application is to receive an equipment PDA for the system or component following Appendix 1-1-A3 of the ABS *Rules for Conditions of Classification (Part 1).*

b) The second application is to receive an ABS CyberSafety PDA for the computer-based system or component following this Guide.

3 Vulnerability Report

The Vulnerability Report is a revision-controlled document that is listed on the ABS CyberSafety PDA or DRL. It is to be made available to the integrator, shipyard, or owner upon request from the OEM. The Vulnerability Report consists of the functionality, Controlled Equipment List, Vulnerability Assessment, installed and/or recommended cybersecurity protective functions (hardware or software), topology drawing of OEM connected components network, potential vulnerabilities associated with any wireless networks and remote connections, and controls associated with wireless networks and remote connections. The Vulnerability Report is used by downstream users in cybersecurity risk analysis and cybersecurity risk profiling to determine if and where to install cybersecurity protective functions to mitigate the cybersecurity risk.

A vulnerability report is required for both an ABS CyberSafety PDA and a Design Review Letter with ABS CyberSafety declaration (DRL).

3.1 Vulnerability Report

The OEM is to report cybersecurity vulnerabilities as reported by sub-suppliers concerning their sub-systems and sub-components provided to the OEM for installation in the computer-based system.

A Vulnerability Report is to be listed for each computer-based system listed on the ABS CyberSafety PDA.

i) The OEM is to submit a Cybersecurity Vulnerabilities Report of the OEM's computer-based system addressing:

a) Cybersecurity Vulnerability Analysis (3/3.3)

b) Description of known OEM cybersecurity vulnerabilities that are not mitigated by the OEM CSPF. If the OEM is planning to introduce mitigating controls, expected implementation description and timeline are to be included.

c) OEM installed CSPF (hardware and software)

d) OEM login requirements to OEM equipment and CSPF:

1) OEM and user passwords requirements:

- Minimum length and complexity (required special characters for OEM's and owner's personnel) and reuse of passwords
- Password lifetime restrictions or time till expiration
- Number of login attempts till disabled or time to retry

e) Computer-based system or component description documents (3/3.5).

f) Sub-supplier functionality descriptions, vulnerabilities descriptions, and topology drawing, as reported by sub-supplier, if any.

g) Sub-supplier's remote connection vulnerabilities, as reported by sub-supplier, if any.

h) OEM's topology drawing (3/3.7).

3.3 Vulnerability Analysis

3.3.1 Items to be Submitted

The OEM is to perform a Cybersecurity Vulnerability Analysis where the OEM is to review each OEM-installed accessible digital endpoint and connected equipment for:

i) Vulnerability Analysis (3/3.3.2), listing CSPF or protections

ii) Controls applied to potential vulnerabilities from access by a digital device or human to each digital endpoint.

iii) Controls applied to potential vulnerability from each digitally-enabled connected component.

iv) Controls applied to potential vulnerability from safety or mission-completion consequence of unauthorized access.

v) Physical or logical protection or monitoring provided or recommended for endpoints.

vi) Controls applied to potential connection to or access by an unidentified or unauthorized digital device (wireless, Internet, via local ports).

vii) Security implemented by OEM for OEM's personnel and digital devices for local and remote access (passwords, two-factor authentication, etc.), both prior to delivery and during field maintenance activities.

viii) Security implemented by OEM for access by end user's personnel and digital devices (limited access privileges, passwords, two-factor authentication, etc.).

ix) Known vulnerabilities of hardware, embedded firmware and software.

x) Tested and OEM approved CSPF installed to mitigate known vulnerabilities:

a) It is recommended that the OEM list of tested and OEM recommended or advised third-party CSPF that is not installed on the equipment or system is included.

b) It is recommended that the OEM list of untested, but OEM-recommended CSPF, if any, which may mitigate known vulnerabilities for post-installation applications is included.

3.3.2 Analysis Process

It is recommended that the OEM follow the Failure Mode and Effects Analysis (FMEA) process to analyze nodes for vulnerabilities listed in Section 3, Table 1 for the computer-based system. Section 3, Table 1 was extracted, in part, from NIST SP 800-82.

Section 3, Table 1 is to be used for the vulnerability analysis of the nodes and connections for the computer-based system or component connection's connections. The OEM may add additional *Risk Contribution Class* items.

TABLE 1
OEM's Vulnerabilities Table

Taxonomy Class ID	*Risk Contribution Class*	*Notes*
F1	List known vulnerabilities in embedded software and firmware and the component each vulnerability is found in. List if found in NIST NVD and the CVSS score. List any CSPF installed by the OEM to mitigate the vulnerability. List any recommended but not installed CSPF. (See Note)	The NIST NVD CVSS assists with protection and criticality determination.
F2	Provide the certificate of any components within the computer-based system that are cybersecurity certified by UL, CSA, or other organization and delivered with an ABS CyberSafety PDA or DRL.	
F3	OEM to review the number of critical and non-critical connections to components or other computer-based systems for cascading events and document results of review and remedies to reduce potential of cascading events.	Probability of critical systems being affected by cascading events increases with the number of critical and non-critical computer-based systems that share common dependency.
F4	OEM to review for vulnerabilities that may increase with connection path complexity and any remedies or controls taken or installed.	Proliferation of endpoints or nodes related to connection complexity (discrete, simple, complex, or Very Large Network (VLN))
F5	OEM to review the potential vulnerabilities introduced with remote OEM connection(s) and OEM controls to mitigate the vulnerabilities.	Supplier remote access maintained by wireless communications (Internet, proprietary satellite)
F6	OEM to review the potential vulnerabilities introduced with local OEM local access and the controls to mitigate the vulnerabilities.	Supplier onboard access to maintain the computer-based system using PCs, portable devices, communications and manual means
F7	OEM to review for potential vulnerabilities associated with insecure or unprotected wireless networks and access, including Wi-Fi, Bluetooth, mobile phone, etc.	Mutual authentication between clients and computer-based system's access points so that wireless clients do not connect to rogue access points and rogue clients do not connect to computer-based system's wireless access point(s).
F8	OEM to review for wireless data encryption requirements, as required.	
C1	OEM to review for unprotected accessible physical endpoints.	RJ45 and USB ports not protected by obscurity or located in locked or restricted access rooms.
C2	OEM to review for unprotected endpoints by cabinet enclosures.	Endpoints not protected by obscurity, restricted access to the containing cabinet.
C3	OEM to review for unprotected endpoints by in situ device, alarm or construct.	Device disconnection from a port alerts the operator of the disconnection.

TABLE 1 (continued)
OEM's Vulnerabilities Table

Taxonomy Class ID	*Risk Contribution Class*	*Notes*
C4	OEM to review for unprotected endpoints not protected by login and password.	Accessible physical port(s) for OEM and/or crew access.
C5	OEM to review for unprotected endpoints not protected by digital device (ID dongle key) carried by personnel to provide identification, two-factor identification (employee number, organizational role), or other methods to prevent humans or digital identities from gaining access to the system.	
ID1	OEM to review for logically unprotected endpoints without some sort of identity challenge: *i)* Identity confirmed by biometric *ii)* Identity confirmed by digital device, ID, key or token *iii)* Identity confirmed by username, password, entry code *iv)* Identity confirmed by documented organizational role *v)* Identity confirmed by monitored communications characteristics, black/white lists, expert system rejection, multifactor	
ID2	OEM to review for digital device accessing endpoint (consider OEM's and owner's personnel): *i)* Access by a digital device not configured for use in accordance with OEM's policy or best practices *ii)* Access by an unscanned digital device for use in accordance with OEM's policy and/or best practices	
O1	OEM to review for computer-based system vulnerabilities if the computer-based system is dependent upon the IT system for any service.	
O2	OEM to review for computer-based system boundary defined as clearly as possible within limitations of scope of delivery.	Does not apply to components.
O3	OEM to review the vulnerabilities associated with unutilized or unused network Ports, Protocols and Services (PPS) within the computer-based system.	It is recommended that unused PPS be disabled or per owner's requirements.
O4	OEM to review for configuration of network switches which may allow for switching loop interfaces storm vulnerability.	i.e., Spanning Tree Protocol (stp), Rapid Spanning Tree Protocol (rstp), or Multiple Spanning Tree Protocol (mstp)
O5	OEM to review vulnerability of any firewalls installed with default configuration or not configured	Note configuration for downstream users to configure.
O6	OEM to review for vulnerabilities of DNS exfiltration and DNS servers not configured to reject untrusted, unknown, or external hosts. Does not apply to non-DNS components.	Identity risk due to misconfigured DNS that may negatively affect OEM system or equipment.
O7	List vulnerabilities that may affect essential services (1/9.1). If none are known, the OEM is to state "No known cybersecurity vulnerabilities affecting essential services are identified at this time".	

Note: In Item F1, the requirement is to enter each component into the National Institute of Standards and Technology (NIST) National Vulnerability Database (NIST NVD) or other recognized national cybersecurity organization to see if the device, software, or firmware is listed. If listed in NIST NVD, then the OEM is to provide the Common Vulnerability Scoring System (CVSS) score or other score from another recognized database of identified software vulnerabilities. If listed, the OEM is to describe mitigation initiatives implemented, if any. If no mitigation initiatives by the OEM are underway or planned, the OEM is to state, "No mitigation initiatives are planned".

If nothing is listed with the NIST NVD or other organizations, the OEM is to state, "No NIST NVD (or other organization) found on ____(date)."

3.5 Equipment Description Document

The OEM is to submit a revision-controlled description of the OT functionality of each computer-based system, component, or equipment under consideration for an ABS CyberSafety PDA or DRL. The OEM is to include the sub-supplier in the functional description and vulnerability analysis and report. At a minimum, the description is to address the following topics:

3.5.1 Computer-based System or Component Functional Description

The functional description may be an operator manual, user manual, or specification detailing the functionality of the computer-based system or component. The items listed below are part of the Vulnerabilities Report.

i) Unique model number or name identifying the computer-based system or component. If the component or computer-based system was previously design assessed, the unique model number or name is to be identical to the previously design assessed computer-based system.

ii) OEM's serial number(s) or equipment tracking identifier of the initial computer-based system.

iii) OT functional description(s) to be submitted:

- *a)* Description of functionality when the system is in a "normal state".
- *b)* Description of functionality when the system is in a "degraded state". May be described in the FMEA, if available. If not available, the OEM is to state, "Degraded state functionality not available".
- *c)* Description of functionality when system has "failed". May be described in the FMEA, if available. If not available, the OEM is to state, "Failed state functionality not available".
- *d)* Overall designation of computer-based system Integrity Level (IL) (see Section 3, Table 1 of the *ISQM Guide*) as assigned by the OEM.
- *e)* Safety FMEA report, if required by other ABS Rules or Guides. If none required, the OEM is to state, "No FMEA required by ABS Rules or Guides".
- *f)* Connection complexity (Discrete, Simple, Complex, Very Large Network) (see 1/9.1.1).

iv) System-wide time source for computer-based systems or the capability to timestamp security events for components.

v) OEM's computer-based system's software version number(s) at the time of Factory Acceptance Test of the initial system.

vi) OEM's firmware version number for computer-based components implemented at Factory Acceptance Test (FAT) of the initial system.

vii) List of digitally-enabled components (Controlled Equipment List) the OEM is supplying for each computer-based system included in the ABS PDA or DRL (Manufacturer, Model number):

- *a)* Network infrastructure components (switches, routers, etc.)
- *b)* Servers detailing Operating System version and Build number
- *c)* Personal Computers detailing Operating System version and Build number
- *d)* PLCs or control system detailing:
  - *1)* Operating System version and Build number
  - *2)* Firmware version
- *e)* HMIs detailing Operating System version and Build number
- *f)* Wireless access points or routers

g) Other network or computer-based system components, networked, serially or wirelessly connected, digitally-enabled and connected devices to be included in the PDA or Design Review Letter with ABS CyberSafety and supplied by the OEM (IOT, IIOT and COTS)

viii) Wireless access point configuration (Wi-Fi, cellular-based broadband, Bluetooth, RF datalink, etc.), if any

ix) A listing of enabled or disabled digital services and ports (Ports, Protocols and Services (PPS)). If PPS are project dependent, state, "PPS are project dependent".

3.5.2 Computer-based System's Connections

i) Describe OEM's cybersecurity measures applied during remote digital connection to the fielded computer-based system:

a) Reference pertinent OEM's cybersecurity policy governance for remote connection.

b) Describe identity controls and verification requirements for authorized access (password length, complexity, etc.) by OEM's personnel from remote locations to client assets.

c) Describe Remote Connections:

1) If no remote connection, state, "No remote connection required".

2) Describe how a remote session is terminated, whether remote sessions are designed to time-out automatically and specify time-out criteria.

3) Specify number of remote concurrent sessions allowed or describe how sessions are limited or controlled.

4) Describe how remotely transferred data is classified and if or how the connection protection is managed – including use of encrypted channels or applications required to protect access to the data transfer operations.

d) Describe monitoring tools (like Security Information and Event Management) or security activities employed for managing unauthorized access detection or protection performed by this computer-based system or component, if any.

e) Describe the process used for performance data and system logs collection and analysis, if any.

f) Describe any intrusion detection or intrusion protection system built into the computer-based system or component, if any.

ii) Describe number of allowed local concurrent sessions and how sessions are limited or controlled and terminated.

iii) The OEM is to remove any undocumented, development or backdoor access accounts before delivery.

iv) The OEM is to disable any basic web servers unless required for computer-based system operation or owner. List any known vulnerabilities associated with web server if enabled.

3.7 Computer-Based System's Topology Drawing

The topology drawings are to be revision-controlled drawing(s) and are part of the Vulnerabilities Report. The requirements in 3/3.7 do not apply for computer-based systems with a discrete or simple connection. If the OEM's networked system, when installed in its final configuration, has less than 10 connected devices in its network segment, then it is permissible to list the nodes and connected devices in a table that includes the information below. The OEM's computer-based system's network topology drawing(s) is to show connections within the OEM's scope of supply including:

i) Digitally enabled components, network infrastructure components. The remote Input and Output (I/O) connections may be shown as a single connection regardless of the number of I/O connections.

ii) HMIs and control panels connected to OT network(s)

iii) Sub-supplier's and contracted and known third-party control and IT equipment connected to OEM's OT network(s). If the sub-supplier has a network segmented from the OEM's OT network, show sub-supplier's connection (gateway) to OEM's network.

iv) IT office network connection(s) to the OEM's network. It is permissible to identify only the network port(s) and not identify specific office equipment, unless the equipment is within the OEM's scope of supply.

v) Data collection connection(s). It is permissible to identify only the network port(s) and not identify data collection equipment, unless the equipment is within the OEM's scope of supply.

vi) Satellite and remote access connection. It is permissible to identify only the network port(s) and not identify remote access equipment, unless the equipment is within the OEM's scope of supply.

vii) Wireless connection point(s), if any.

viii) Show CSPF (routers, programmed switches, etc.) installed.

ix) Network monitoring system installed by the OEM or OEM's sub-supplier.

a) If network monitoring is not installed by the OEM or OEM's sub-supplier, the OEM is to identify and provide one or more inaccessible RJ45 ports for each network segment for connection of network monitoring system in the future, if network switches are within the OEM's scope of supply.

b) The port(s) for future network monitoring are to be identified, but not the ports that are permanently disabled.

3.9 Anti-malware Scans and Software Backups

i) The OEM is to perform an anti-malware scan at FAT of every computer-based system and make the results available for ABS review upon request. The expected information, at minimum, is:

a) Name of vessel or offshore asset

b) Date of the scan

c) Anti-malware software name

d) Virus definition number

e) Scan Report. If the scan reports known code as potential malware, note that it is expected and state the reason.

ii) Malware-free software is to be backed up in a safe location with parameters by OEM or may be provided to owner. The Surveyor may request to be informed of the location of backed-up software at the audit.

5 Hardware and Software Updates

The ABS CyberSafety PDA Certificate is associated with described Cybersecurity Protective Functions or controls (CSPF) and components of the computer-based system. All computer-based systems ordered with an ABS CyberSafety PDA Certificate are to be delivered with components described within the ABS CyberSafety PDA documentation.

- Subsection 3/5 is applicable to the ABS CyberSafety PDA only.
- Refer to Appendix 1-1-A3 of the ABS *Rules for Conditions of Classification (Part 1)* for applicable PDA requirements associated with the computer-based system hardware and equipment.

5.1 Updates and Additions to the PDA Defined Computer-Based System

The installation of newer, more capable, or supportable components with new hardware and software within a computer-based system is anticipated, and minimally requires the submittal of a PDA revision request if the OEM is a certified Service Provider. These updates may resolve discovered cybersecurity vulnerabilities, fix software bugs, or add beneficial functionality. Computer-based system updates are listed below to keep the ABS CyberSafety PDA current for various hardware or software changes or updates to the computer-based system:

i) Additions or changes to the hardware PDA defined computer-based system (3/5.3):

a) The owner or shipyard may require additional components to be connected to the PDA defined network and the shipyard requires the computer-based system be delivered with ABS CyberSafety PDA. The OEM can either apply for a new ABS CyberSafety PDA (Subsection 3/1) or apply for a DRL (3/5.3) if acceptable to the shipyard for a unique install of the additional component(s).

ii) Hardware replacement:

a) Replacement-in-kind of network architecture component does not require notification of ABS (same manufacturer, same model)

b) Replacement-in-kind of control system component does not require notification of ABS (same manufacturer, same model)

c) Replacement-not-in-kind of computer-based system's digitally-enabled component, HMI, Personal Computer, network infrastructure component, or servers requires a new equipment PDA to be requested and updates or revision to the ABS CyberSafety PDA (see 3/5.5).

ii) Software or firmware updates. See 3/5.5 in all cases for all digitally-enabled components.

5.3 Certified Service Providers with Component Additions to a PDA

The OEM may install additional components (both digitally-enabled process equipment, CSPF or network infrastructure) connected to the computer-based system's PDA-defined network as required by the specification for a specific vessel, the OEM is to:

i) Contact ABS for a DRL for the specific installation (Subsection 3/1).

ii) Update and submit the Vulnerability Report (3/3.1) and reference previous PDA certificate number.

iii) The *Marine Vessel Rules* and ABS *Rules for Conditions of Classification (Part 1)* may apply and have additional requirements.

5.5 Product Design Assessment Software Updates

Software or Firmware Update to a Component within the Computer-based System:

i) Submit a PDA revision application form (3/1.1.2)

ii) Update and submit the Vulnerability Report (3/3.1)

5.7 Design Review Letter Updates

An update to a system or component with a DRL requires a new DRL. This includes both software and firmware updates.

SECTION 4 Surveyor Audits and Type Tests for ABS CyberSafety

1 ABS CyberSafety PDA Type Test

Equipment for an ABS CyberSafety PDA is to be type tested by the OEM for ABS CyberSafety. This type test is to be witnessed by ABS and may be performed on board or at the factory. Type testing per Appendix 1-1-A3 of the ABS *Rules for Conditions of Classification (Part 1)* may also apply to the computer-based system or component.

The ABS CyberSafety PDA has an ABS CyberSafety type test on the first instance of the component or computer-based system and may have other type testing required by the Rules associated with equipment PDA. The DRL does not require ABS CyberSafety type testing.

1.1 ABS CyberSafety Type Test

The ABS CyberSafety type test consists of the following:

i) Digitally-enabled components match the topology drawing and/or Controlled Equipment List.

a) Items to be verified are:

1) Computer-based System's control system components (PLC, I/O cards, network, etc.)

2) Network equipment (wired and wireless), within the scope of supply.

3) Network infrastructure components, within the scope of supply.

ii) Computer-based system software current version number(s) are displayed with documentation provided to Surveyor.

iii) OEM installed CSPF (hardware and software) software version number(s) with documentation provided to Surveyor.

iv) Accessible physical ports (USB and RJ45) are indicated to the Surveyor, either on the component or on the drawing, and these ports are blocked or disabled.

3 ABS CyberSafety OEM Audit

3.1 ABS Certified Service Provider Initial and Annual Audit

After engineering review is complete and all comments are closed, OEM's who are seeking Service Provider certification are to proceed with the audit of the following items:

i) CSO audit finding or reviews [2/3.3.2v)]

ii) CSO corporate technical risk review tolerance and technical risk mitigation evaluation documents [2/3.3.2v)]

iii) Incident Response Plan including the recovery procedure for the computer-based system under consideration for the ABS CyberSafety PDA or DRL [2/3.3.3iv)a)]

iv) Records of tabletop exercises focused on client recovery from a cyber incident for the computer-based system under consideration [2/3.3.3iv)b)]

v) Any changes to cybersecurity policies, procedures, change management and configuration control since the last ABS audit [2/3.3.4]

vi) Demonstrate Change Management and Configuration Control system [2/3.3.7]

vii) Anti-malware scan reports [3/3.9]

viii) Software backup [3/3.9ii)]

APPENDIX 1 Check List for OEM Company and Equipment for ABS CyberSafety

1 OEM Service Provider Certificate Check List

Appendix 1, Table 1 contains the requirements and references for an OEM seeking to be registered as a Service Provider.

TABLE 1
OEM Company Requirements for Service Provider Check List

Reference	*Requirement*
2/3.3.1	OEM to state foundational cybersecurity standard used by OEM
2/3.3.2	**Cyber Security Office (CSO)**
2/3.3.2i)	Mission statement of CSO and goals for the computer-based systems
2/3.3.2ii)	Name or titles of the CSO members
2/3.3.2iii)	Roles and responsibilities of CSO members, including approvals and authorities
2/3.3.2iv)	OEM's organizational chart showing the CSO
2/3.3.2v)	Upon request: CSO audit records
2/3.3.2vi)	Upon request: Corporate technical risk tolerance and technical risk evaluation documentation
2/3.3.3	**OEM's Incident Response Team Organization (IRT)**
2/3.3.3i)	Organization, office, or persons who are responsible for providing support to clients who require assistance to recover form a cyber-related software failure
2/3.3.3ii)	Incident Response Plant with recovery procedure
2/3.3.3iii)a)	OEM to submit: Incident Response Policy and procedure
2/3.3.3iii)b)	OEM to submit: Mission statement of the IRT
2/3.3.3iii)c)	OEM to submit: Roles and responsibilities of IRT members, including approvals and authorities
2/3.3.3iv)a)	Upon request: Incident Response Plan for the computer-based system
2/3.3.3iv)b)	Upon request: Indication of periodically performing tabletop exercises focused on client recovery from a cyber incident
2/3.3.3iv)c)	Upon request: Finding of any incident response investigation of a reported computer-based system failure, with approved remedies and implementation timeline, or the procedure for such investigation
2/3.3.4	**OEM's Cybersecurity Policies and Procedures**
2/3.3.4i)a)	Physical and access security
2/3.3.4i)b)	Acceptable use policy of OEM’s digital devices, including portable devices
2/3.3.4i)c)	Digital access, registration, and de-registration of OEM’s personnel and contractors
2/3.3.4i)d)	Protection of information (during processing, storage, and data breach response)
2/3.3.4ii)a)	Remote access (into OEM's network)
2/3.3.4ii)b)	Use of wireless and mobile devices

Reference	*Requirement*
2/3.3.5	**OEM's Internal Risk Management**
2/3.3.5i)	If not ISO 27001 Certified and upon request: Enterprise and product cyber risk assessment policies and procedures
2/3.3.5ii)	If not ISO 27001 Certified and upon request: Documents describing periodic cyber risk assessment of enterprise business systems with consideration of controls in place to manage identified risks.
2/3.3.5iii)	Upon request: Documents describing periodic technical cyber risk assessments of products, including risks identified, risks tolerated or accepted, controls embedded in products to manage identified risks, and controls recommended for managing risks after product implementation.
2/3.3.6	**Cybersecurity Training**
2/3.3.6i)a)	Cybersecurity awareness and training topics
2/3.3.6i)b)	Titles of provided training topics and titles of personnel who periodically receive the training
2/3.3.6i)c)	Records of logs of completions of training by personnel and contractors
2/3.3.6i)d)	On-boarding training topics for new personnel (if different from above)
2/3.3.6i)e)	Schedule of periodic refresher cybersecurity and change management policies and procedure training
2/3.3.7	**OEM Change Management and Configuration Control**
2/3.3.7i)	Change Management policy and/or procedure
2/3.3.7ii)	Tracking of change management from request through implementation
2/3.3.7iii)	Software change management program or practices to manage inherent evolutionary conditions
2/3.3.8	**Third Party Involvement in Programming of the OEM's Software**
2/3.3.8i)	State if the third party uses the same policies and procedures as the OEM
2/3.3.8ii)	Submit the 2/3.3.1 through 2/3.3.7 documents if the documents are different from the OEM
2/3.3.8iii)	OEM to detail how the OEM receives, verifies, and tests software obtained from third parties
2/3.5	**Copies of Certificates**
2/3.5	Copies of ISO-9001, ISO-27001, ISA-62443, or other cybersecurity certificates

3 OEM Requirements Non-Service Provider Check List

Appendix 1, Table 2 contains the requirements and references for OEM not seeking to be registered as a Service Provider.

TABLE 2
OEM Company Requirements not Seeking Service Provider Certification Check List

Reference	*Requirement*
2/5.1i)	OEM to state foundational cybersecurity standard
2/5.1ii)	Person, organization, or office responsible for cybersecurity of the enterprise and products
2/5.1iii)	The composition and responsibilities of the cybersecurity Incident Response Team
2/5.1iv)	OEM Cybersecurity Policies and Procedures detailing:
2/5.1iv)a)	Training in cyber hygiene and specialized cybersecurity functions
2/5.1iv)b)	Physical access security
2/5.1iv)c)	Digital access, registration, and de-registration of OEM's personnel and contractors
2/5.1iv)d)	Acceptable Use Policy of OEM’s digital devices and portable devices
2/5.1v)	Internal review of technical cybersecurity risk inherent to the OEM’s products
2/5.1vi)	Documents indicating control of product change and configuration
2/5.1	Copies of ISO-9001, ISO-27001, ISA-62443, or other cybersecurity certificates (2/3.5)

5 Equipment Level Requirements Check List

Appendix 1, Table 3 contains the requirements and references for equipment requirements for either an ABS CyberSafety PDA or a Design Review Letter with an ABS CyberSafety declaration.

TABLE 3
Equipment Level Requirements for PDA or DRL Check List

Reference	*Requirement*
3/3.1	**Vulnerability Report**
3/3.1i)a)	Vulnerability Analysis (see 3/3.3)
3/3.1i)b)	Description of known OEM cybersecurity vulnerabilities that are not mitigated by the OEM CSPF
3/3.1i)c)	OEM installed CSPF (hardware and software)
3/3.1i)d)	OEM login requirements to OEM equipment and CSPF
3/3.1i)e)	Computer-based system or component description documents (normal state- required, degraded and failed states – if available) (see 3/3.5)
3/3.1i)f)	Sub-supplier functionality description, vulnerabilities description, and topology drawings as reported by sub-supplier, if any
3/3.1i)g)	Sub-supplier remote connection vulnerabilities, as reported by sub-supplier, if any
3/3.1i)h)	OEM's topology drawing (see 3/3.7)