GUIDE FOR

CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES

ABS CyberSafety^{TM} VOLUME 2
SEPTEMBER 2016

NOTICE NO. 2 – June 2018

The following Changes were approved by the ABS Rules Committee on 14 June 2018 and become **EFFECTIVE AS OF 15 JUNE 2018.**

(See http://www.eagle.org for the consolidated version of the Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafety^{TM} Volume 2 2016, with all Notices and Corrigenda incorporated.)

Notes - *The date in the parentheses means the date that the Rule becomes effective for new construction based on the contract date for construction. (See 1/5.5)*

FOREWORD

(Revise sixth paragraph, as follows:)

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.

SECTION 1 INTRODUCTION TO THE GUIDE

(Revise Subsection 1/3, as follows:)

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 *(1 June 2018)*

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.

(Revise Subsection 1/7, as follows:)

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[1].

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**.

11 Definitions *(1 June 2018)*

(Add definitions of "CS-Ready" in Subsection 1/11, as follows:)

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.

SECTION 3 ASSESSMENT OF CYBERSECURITY IMPLEMENTATION FOR AN ORGANIZATION AND ITS ASSETS

3.3 CS1 – Informed Cybersecurity Implementation (Basic)

(Revise Subparagraph 3/3.3.1, as follows:)

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.

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

(Revise Item i) of Subsection 3/5, as follows:)

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.

(Add new Section 8, as follows:)

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.