GUIDE FOR

CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES

ABS CyberSafety™ VOLUME 2 SEPTEMBER 2016

NOTICE NO. 1 – June 2018

The following Changes were approved by the ABS Rules Committee on 1 June 2018 and become **EFFECTIVE AS OF 1 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™ 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)*

SECTION 1 INTRODUCTION TO THE GUIDE

3 Application and Scope

(Revise Paragraph 1/3.1, as follows:)

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.

(Following text remains unchanged.)

5 Certification

(Revise Paragraph 1/5.1, as follows:)

5.1 General *(1 June 2018)*

(Preceding text remains unchanged.)

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.

(Following text remains unchanged.)

(Revise Footnote 3, as follows:)

[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.

(Revise Item vii) of Paragraph 1/5.3, as follows:)

5.3 Certification Process *(1 June 2018)*

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

(Revise Paragraph 1/5.5, as follows:)

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.

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.

(Revise Subsection 1/7, as follows:)

7 Notation *(1 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.

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

11 Definitions *(1 June 2018)*

(Revise definitions of "CMSC" and "CyberSafety Management System Certificate (CMSC)" in Subsection 1/11, as follows:)

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.

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.

(Add new Subsection 1/15, as follows:)

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.*
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.*

Cybersecurity Management System – Functional Description Document (CMS-FDD)		
No.	*Title*	*Description*
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 3 ASSESSMENT OF CYBERSECURITY IMPLEMENTATION FOR AN ORGANIZATION AND ITS ASSETS

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

5 Applicability of Notations and Certifications *(1 June 2018)*

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.

(Revise Subsection 3/11, as follows:)

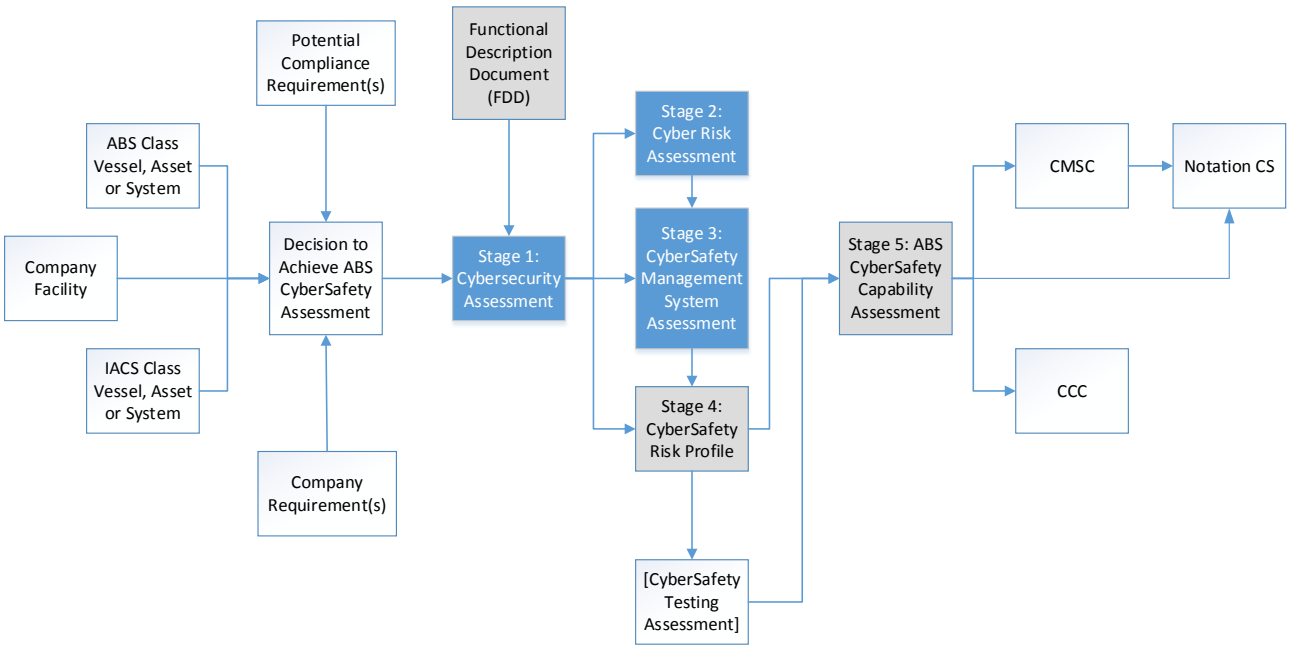
11 Capability Assessment Process *(1 June 2018)*

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.

(Revise Section 3, Figure 2, as follows:)

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



SECTION 4 REQUIREMENTS FOR CERTIFICATION

(Revise Subsection 4/3, as follows:)

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

(Preceding text remains unchanged.)

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.

(Following text remains unchanged.)