



GUIDANCE NOTES ON

THE APPLICATION OF CYBERSECURITY PRINCIPLES TO MARINE AND OFFSHORE OPERATIONS

VOLUME 1: CYBERSECURITY

FEBRUARY 2016

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

**Copyright © 2016
American Bureau of Shipping
ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA**

Foreword

ABS recognizes that automation methods – and increasingly, autonomy – have penetrated nearly all aspects of shipboard and platform systems. Because these systems control multiple aspects of asset, ship or platform operations, they become integral parts of system and operational safety.

ABS supports our community by compiling best practices, deriving new methods, and developing the standard for marine and offshore cybersecurity in a commitment to safety and security of life and property and preservation of the environment.

This document is Volume 1 of the ABS CyberSafety™ series. It provides best practices for cybersecurity, as a foundational element of overall safety and security within and across the marine and offshore communities. The best practices are meant to provide insights for operations, maintenance and support of cyber-enabled systems, to better assure safety and security in those systems.

These Guidance Notes become effective on the first day of the month of publication.

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

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



GUIDANCE NOTES ON

THE APPLICATION OF CYBERSECURITY PRINCIPLES TO MARINE AND OFFSHORE OPERATIONS

VOLUME 1: CYBERSECURITY

CONTENTS

SECTION 1	General	1
1	Objective	1
2	Application	1
3	Cybersecurity	1
4	Definitions	1
SECTION 2	Cybersecurity Program Development	3
1	Introduction	3
2	Intersection of Cybersecurity and Safety	3
3	Best Practices	4
4	Structure for Best Practices	6
4.1	Basic Capability	6
4.2	Developed Capability	6
FIGURE 1	Basic Capability Set	4
FIGURE 2	Developed Capability Set	5
SECTION 3	Best Practices and the Application of Cybersecurity Principles to Marine and Offshore Operations: Basic Capability Set	7
1	Exercise Best Practices	7
1.1	References	7
2	Build the Security Organization	8
2.1	References	8
3	Provision for Employee Awareness and Training	8
3.1	References	9
4	Perform Risk Assessment	9
4.1	References	9
5	Provide Perimeter Defense	10
5.1	References	10
6	Prepare for Incident Response and Recovery	11
6.1	References	11

7	Provide Physical Security	12
7.1	References	12
8	Execute Access Management	12
8.1	References	13
9	Ensure Asset Management.....	14
9.1	References	14

SECTION 4 Best Practices and the Application of Cybersecurity Principles to Marine and Offshore Operations: Developed Capability Set..... 15

10	Perform Policy Management.....	15
10.1	References	15
11	Provide Standards and Governance.....	15
11.1	References	16
12	Provide and Guide Cybersecurity Hygiene.....	16
12.1	References	17
13	Gather and Use Threat Intelligence.....	17
13.1	References	17
14	Perform Vulnerability Assessment.....	17
14.1	References	18
15	Perform Risk Management	18
15.1	References	19
16	Provide Data Protection	19
16.1	References	20
17	Protect Operational Technology (OT).....	20
17.1	References	21
18	Perform System and Security Continuous Monitoring (SCM)	22
18.1	References	22
19	Plan for Disaster Recovery (DR).....	22
19.1	References	23
20	Provide Unified Identity Management.....	23
20.1	References	23
21	Perform System, Software, and Application Test	24
21.1	References	24
22	Perform System and Application Patch and Configuration Management	24
22.1	References	25
23	Execute Change Control as an Enterprise Process	25
23.1	References	25

SECTION 5 Best Practices and the Application of Cybersecurity Principles to Marine and Offshore Operations: Additional Capabilities in the Mature Organization..... 26

24	Execute Capital Planning and Investment Control (CPIC)	26
24.1	References	26
25	Implement Architecture Management.....	26
25.1	References	27

26	Provide Secure Engineering	27
26.1	References	28
27	Exercise Communications Management	28
27.1	References	29

This Page Intentionally Left Blank

Copyright American Bureau of Shipping
Provided by IHS
No reproduction or networking permitted without license from IHS



SECTION 1 General

1 Objective

These Guidance Notes provide cybersecurity best practices and recommendations to marine and offshore organizations, and they are intended to enable members of the marine and offshore communities to take verifiable steps to protect an asset, its cyber-connected systems, its personnel, and its information from cyber intrusions. The overarching ABS cybersecurity guidance program provides these Guidance Notes as “Volume 1: Cybersecurity”.

2 Application

These Guidance Notes apply to cybersecurity implementations for ships, platforms, and support facilities, and support a practical application of the engineering and operations of cyber-enabled systems in the marine and offshore environments.

3 Cybersecurity

Security is a critical enabling function for an organization, company, agency or unit. Therefore, security is implemented to protect critical assets of all types, ranging from staff, equipment and facilities to computerized systems. Security implementations themselves are assets, requiring the same security protections that they in turn offer to the larger organization. Most organizations arguably understand the need for protecting and monitoring cyber-linked business support and control systems. Even so, the breadth and complexity of protecting such systems may present a daunting challenge to many organizations that do not have a comprehensive picture of cybersecurity.

Successful cybersecurity is the result of a complex series of related and interdependent work efforts that intersect so as to provide protections that are functional and enduring in the face of challenges presented by geography, technological evolution, and shifting human resource capabilities and deployment.

A thorough understanding of the protected organization, its supporting physical and intellectual assets, and the needs and capabilities of its people provides the foundation for a structured cybersecurity program. That security program expectedly changes and develops as it orders and prioritizes requirements, develops its capabilities, builds its functional capabilities, and aligns itself with the organization, its mission and its goals. Because every organization is unique in its needs, priorities and limitations, every security program is also unique in its protective functionality, sequence of areas protected, and protection timetables.

This document, “Volume 1: Cybersecurity”, of the ABS CyberSafety™ series, appreciates and accommodates the unique characteristics required to build and maintain a cybersecurity program. The Guidance Notes offer guidance that attempts to represent due care and due diligence in cybersecurity.

4 Definitions

Capability: The ability to execute a specified course of action. (Adapted from: CNSSI 4009, Joint Publication 1-02. Source: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf)

CyberSafety: Guidelines and standards for computerized, automated, and autonomous systems that ensure those systems are designed, built, operated, and maintained so as to allow only predictable, repeatable behaviors, especially in those areas of operation or maintenance that can affect human, system, enterprise or environmental safety. CyberSafety is required for the deterministic behaviors found in engineered functional assurance, and it includes software integrity management to manage technical risk in software-intensive systems.

ABS CyberSafety™: Measurable implementation of CyberSafety that tailors cybersecurity and systemic safety to assets in order to enable and encourage risk-based asset management as a systemic outcome. ABS CyberSafety™ will provide deterministic outcomes when implemented within managed environments that include appropriate processes, policies, system test and audit, and data management.

Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. (Adapted from: *CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009*. Source: <https://niccs.us-cert.gov/glossary>)

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. (From: *NIST SP 800-53 Rev 4 (glossary)*. Source: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>)

Operational Technology (OT): An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes. (Adapted from: *NIST SP 800-53 Rev 4*. Source: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>)

Smart Asset: Marine and offshore assets built with significant degrees of automated control of vessel or platform operations, system management and monitoring, and data communications. Automation provides labor-saving capabilities; augments human strength; augments human decision-making and error-checking processes; provides operational situational awareness; enables multiple simultaneous system control and management; and provides for controlled data storage. A Smart Asset may possess automated or autonomous processes that operate without routine human intervention.



SECTION 2 Cybersecurity Program Development

1 Introduction

ABS recognizes that automation is pervasive in shipboard and platform systems. Because automated systems control multiple critical aspects of marine and offshore assets, ship and platform operations, these systems are now subject to the same safety-related concerns as is any other critical vessel feature.

“Volume 1: Cybersecurity” addresses cybersecurity practices for systems, ships and platforms as part of the ABS CyberSafety™ series. Beginning with best practices, the series will help owners, operators and regulators to verify the various automated systems found at sea and ashore can neither cause harm to personnel, nor compromise system integrity or operations.

Cybersecurity is the first area to be addressed in building secure and safe systems. As the series matures and is implemented by ship and platform owners, operators and crews, additional products will be provided to support self-assessment, self-test, and self-audit. The series will provide test, data management, software assurance, automated systems (i.e., robotics and safety-critical systems) and autonomous system guidance and technical direction. Appendices to the ABS CyberSafety™ document series will provide strategy, policy, processes, and safety assessment tools, checklists and audit templates.

2 Intersection of Cybersecurity and Safety

The marine and offshore environments include pervasive information technology (IT), and extensive and growing numbers of cyber-physical systems (CPS). These systems provide labor multipliers to assist the captain and crew in operating the ship effectively and efficiently, providing machinery and ship controls, monitoring and alerting. Navigation, propulsion, ship control (maneuvering), system management, cargo management, and safety sensors and alarms – all supplement people and assist people while providing functions to keep people working and out of harm’s way. Both IT and CPS systems must operate as expected if they are to support the crews’ processes and procedures.

Ship and platform automated systems are now connected in ways never before considered. Crews, vessel operators, platform or facility managers, and original equipment manufacturers (OEMs) want remote access, greater on-station function, frequent reporting from sensors, and new types of data and functions. To support these requirements, many control systems are coupled via industry-standard communications and networking, interfaced to Internet-connected networks, and operated in multiple modes unanticipated at system design. The result is that general-purpose systems are frequently connected to special purpose process control systems, exposing control systems to security incidents that can have operational consequences.

A cybersecurity incident on a ship, on a platform, or within a facility, might result from system fault or failure, operator error or inaction, inadvertent conflicts in incompatible software, or deliberate malfeasance or malice. Any such incident may result in intrusion or malfunction in a general purpose network, resulting in a cascading failure that can spread into ship or platform CPS to cause unexpected consequences for any number of systems.

Because of system interconnections, a CPS failure might even bring about ship-wide failures that can, in turn, affect the surrounding community and environment. It is the responsibility of mariners and seafarers to know their systems, know their interfaces, know how both work together, how they might fail, and the failure consequences.

Cybersecurity and software integrity management are both increasingly important to the broader understanding of our systems, our software, and our overall system safety. Cyber-enabled systems and gear are all around us. The security aspects of highly automated, integrated, computerized gear must be well understood, especially when considering the safety-related impacts of security on both individually controlled systems and linked systems.

The first step to improved cybersecurity is knowledge of the approaches developed and implemented by other practitioners in the field who have gained and shared valuable experiences and lessons learned. This document contains practical information that has been researched and vetted for application to the marine and offshore industries. It is a collection of best practices deemed to be useful both to novice specialists just beginning to establish cybersecurity programs, and to seasoned experts who want to review the best practices of others in order to continue improving their cybersecurity programs and implementations.

3 Best Practices

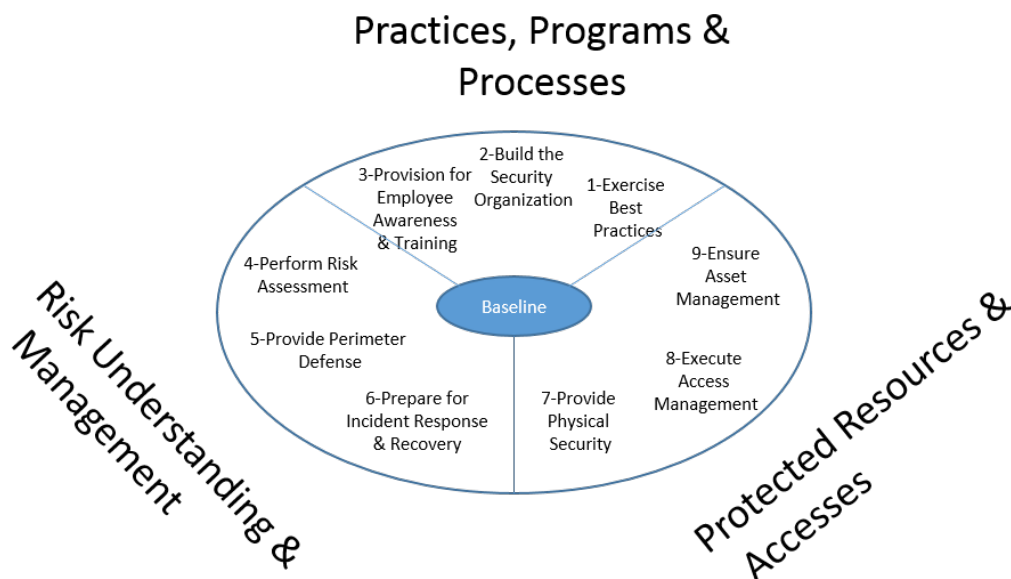
ABS CyberSafety™ is the ABS process for adding cybersecurity rigor to both the operational systems aboard ships and platforms, and to the linked business systems that support their missions. The best practices in these Guidance Notes will help the reader understand how to frame and prioritize cybersecurity work efforts in going about building rigor, security and safety into systems.

This volume concentrates on the establishment of Basic and Developed Capabilities that fully enable a cybersecurity work effort. In this context, a Capability is broad in that it includes people, systems, data, and processes. An organization builds these Capabilities incrementally based on security needs, staff competencies, available acquisition resources, and organizational maturity in cybersecurity.

Capabilities built according to this method become the organization's support framework for security controls, policies and procedures. The program laid out in this way becomes an overlay that can be used with any compliance framework's security controls, or it can be a measurable compliance set in its own right. The arrangement of the Capabilities is consciously structured to provide supportability and life cycle management inside the personnel structures built and maintained by the organization, for both cybersecurity and system safety.

Section 3, Figure 1 illustrates the most basic Capabilities that are required to build a cyber-safe program to support cyber-secure systems. At the core of the program are the baseline controls and tasks – the information technology fundamentals – commonly employed to support a business or operational (shipboard, offshore or port facility) system. Surrounding this baseline are Capabilities needed to shape an environment that is ready to sustain a robust cybersecurity program.

FIGURE 1
Basic Capability Set



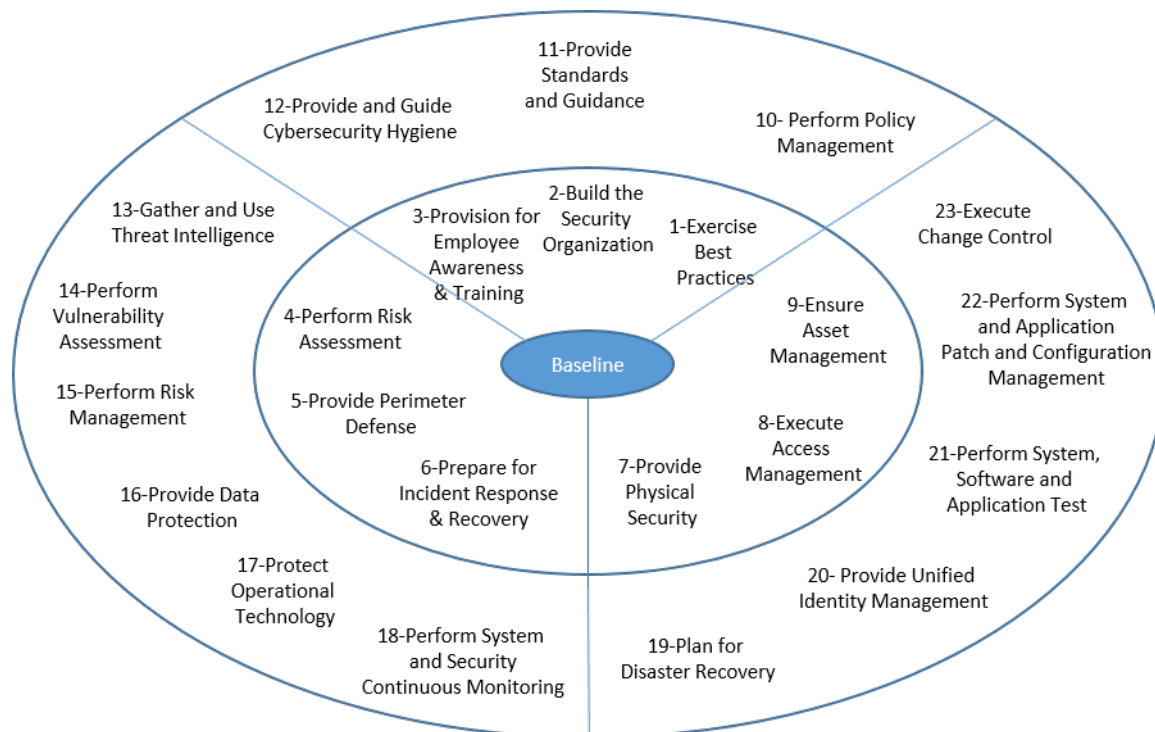
The nine Basic Capabilities shown should be developed and implemented within the organization, and should be evident as fully documented, employed, supported, and maintained.

These Capabilities are critical to establishing a viable cybersecurity program, and they are judged by ABS to be the minimum set required in order to evaluate, analyze, and provide a measurable initial status of cybersecurity in automated systems and their host organization(s). The nine Capabilities are arranged in more general divisions that can aid in organizing and understanding the functions, factors which may be more important in smaller, or less mature, organizations that must be relatively more careful about expenditures and personnel assignments.

Capabilities are the primary elements supporting a cybersecurity program. Capabilities enable organizations to perform complete cybersecurity tasks that are interrelated with other software and systems engineering tasks. Prioritization of the security tasks, and the Capabilities that enable those tasks, may change based on an organization's available resources for performing the tasks and its installed base of assets requiring protection. In support of those imperatives, "Volume 1: Cybersecurity" provides a way to approach prioritization in a scalable, measurable, and complete way.

Section 3, Figure 2 indicates how this cybersecurity program extends the foundational Basic Capability Set into a more functionally complete Developed Capability Set. These additional Capabilities build on the Basic Capability Set to provide both depth and breadth in the three functional divisions. The purpose of this layered approach is that it enables the builder of a cybersecurity program to select and implement Capabilities in a way that best satisfies the needs and constraints of the supported organization or asset.

FIGURE 2
Developed Capability Set



The outside layer of the Developed Capabilities Set provides relative completeness to an organization having a need, a level of maturity, and available resources to establish a well-formed cybersecurity system. A third set of capabilities (not shown), provides guidance for a fully formed, highly capable cybersecurity system.