GUIDANCE NOTES ON

THE APPLICATION OF CYBERSECURITY PRINCIPLES TO MARINE AND OFFSHORE OPERATIONS

ABS CyberSafety™ VOLUME 1

SEPTEMBER 2016

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

ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA

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.

These Guidance Notes have been updated to align with Volume 2 of this series, ABS *Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafety™ Volume 2*. It has been expanded to reflect the full set of 37 Capabilities that define competencies for the ABS CyberSafety™ environment.

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

ABS CyberSafety™ VOLUME 1

CONTENTS

This Page Intentionally Left Blank

SECTION 1 General

1 Objective *(1 September 2016)*

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 within the overall program context of ABS CyberSafety™.

The principal objective of this document is to support the ABS *Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafety™ Volume 2* by providing a readable summary of the practices needed for CyberSafety. The best practices in these Guidance Notes provide the basis for the reader to understand the specifications, and the subsequent requirements, within each of the Capabilities listed in this document. In that way, Volume 1 serves as an introductory document for the more detailed Volume 2.

2 Application *(1 September 2016)*

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

Note: The general term "vessel" used throughout these Guidance Notes denotes a ship, a barge, an offshore asset or facility, or any other floating or fixed structure.

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 Companies 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 Company, 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 Company, its mission and its goals. Because every Company 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 *(1 September 2016)*

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 seek to shape those systems to be 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 *(1 September 2016)*

2.1 Dependence on Software and Automation

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 cause 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.

2.3 Applicability

Cybersecurity, as envisioned and presented in this document, protects against both malicious and inadvertent sources. User error, accidents, hardware failures, software faults, or negligence must all be designed or allocated out of the system, in addition to designing out potential avenues of intentional attacks, with the goal of making the systems being protected resilient and safe for personnel, the ship or asset, and for the environment.

The objectives and/or implications of either inadvertent or malicious cyber-system faults, errors or attacks can vary widely. If malicious, system control is just one possible consequence of hostile actions. Data exfiltration and intellectual property theft are known potential risks. Use of a system as a "jumping off point" for other attacks, whether against other Company assets or against outside organizations, is another possible outcome.

Of equal importance, however, are the implications of user error or negligence, and either man-made or natural disasters on the information and control systems built into ships or at-sea assets. Far more opportunities for human error or inadvertent system faults present themselves in system operations than designers or builders expect; it is the training and documentation of processes and procedures that help insure against these categories of errors. For natural disasters, we plan for business continuity, designing resilience into systems, processes and assets.

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 *(1 September 2016)*

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. A Company 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 Company'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 Company, for both cybersecurity and system safety.

Section 2, 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 *(1 September 2016)*

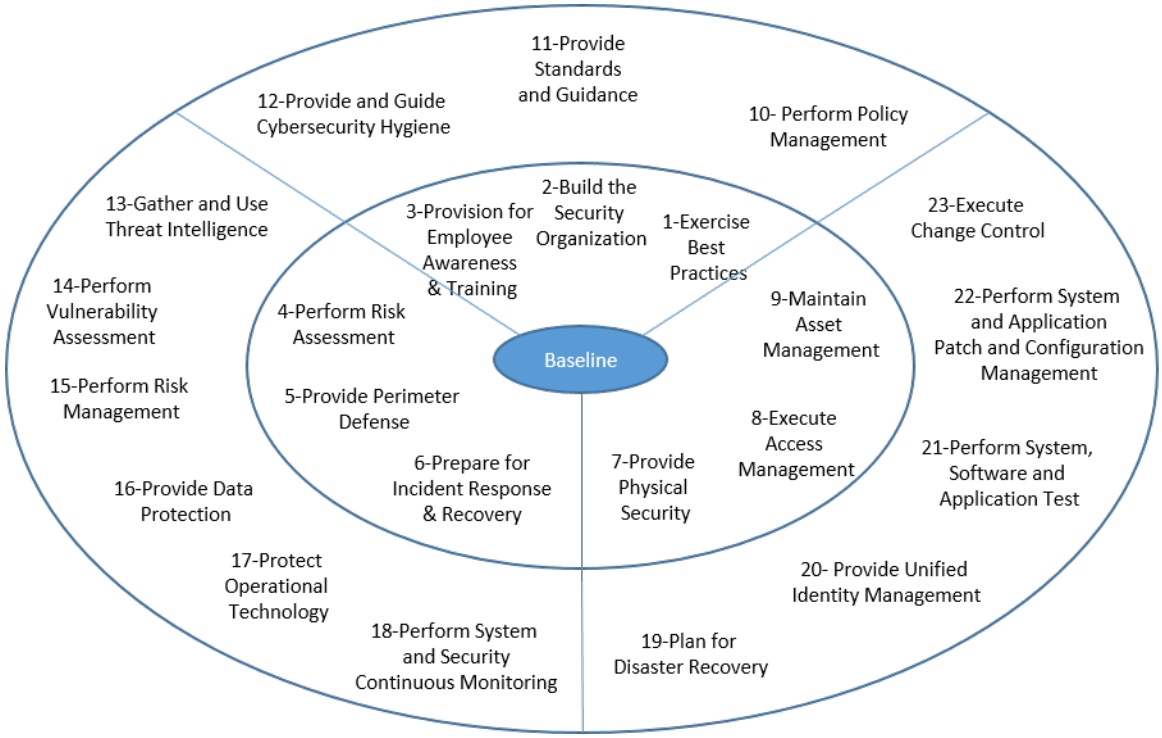
The nine Basic Capabilities shown should be developed and implemented within the Company, and should be evident as fully documented, employed, supported, and maintained.

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, companies that must be relatively more careful about expenditures and personnel assignments.

Capabilities are the primary elements supporting a cybersecurity program. Capabilities enable companies 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 a Company'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 2, 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 *(1 September 2016)*

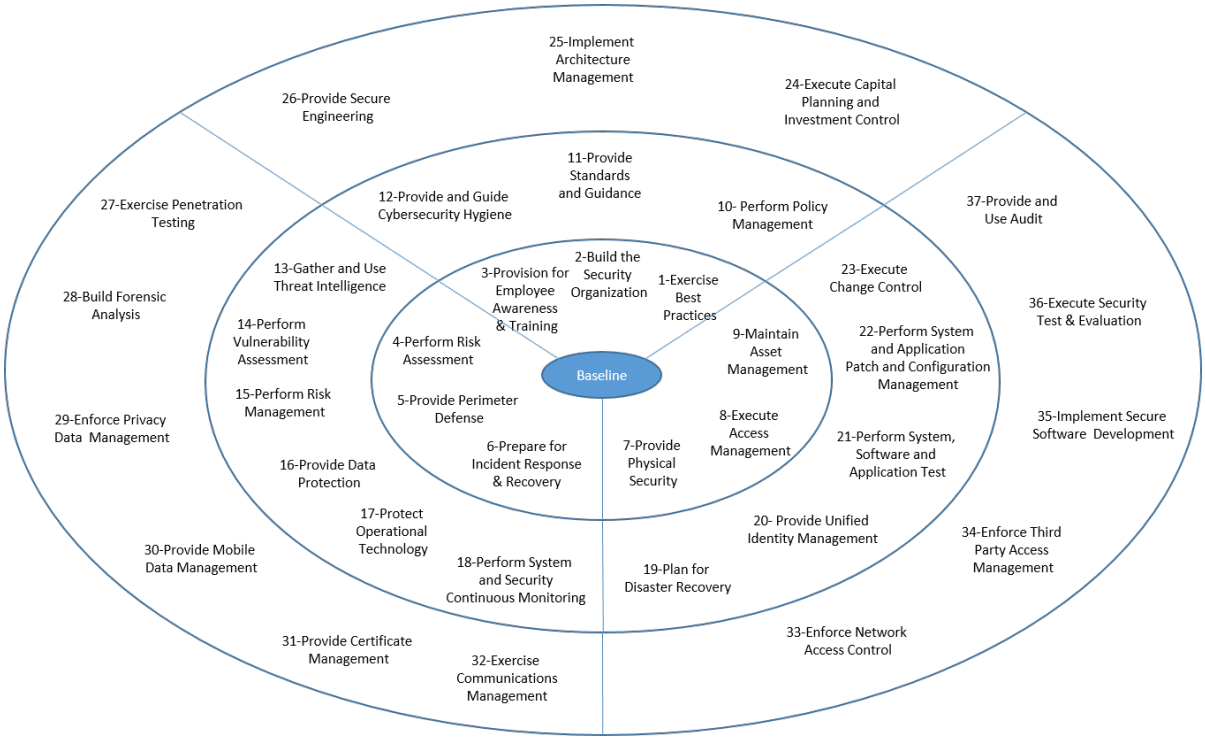


The outside layer of the Developed Capabilities Set provides relative completeness to a Company having a need, a level of maturity, and available resources to establish a well-formed cybersecurity system. A third set of capabilities provides guidance for a fully formed, highly capable cybersecurity system.

Section 2, Figure 3 presents the model fully, showing the Integrated Capability Set. This third set of components provides for capabilities needed to manage and operate combined task sets in a complex environment.

Single capabilities from the Basic or Developed sets can be self-contained. The Integrated set builds capabilities in the Company that require multiple derivative inputs to generate full value for the Company.

FIGURE 3
Integrated Capability Set *(1 September 2016)*



4 Structure for Best Practices *(1 September 2016)*

Below are the Best Practices that ABS associates with the layers of cybersecurity capabilities minimally needed to protect companies, ships, and offshore assets. These Best Practices are compiled from across multiple industries, multiple government reports, individual recommendations, and white papers.

Not all best practices fit every situation, operational context, or application; even so, the listed practices are primarily based on lessons learned by implementers that have paved the way in cybersecurity program development and can arguably enable a practitioner to stand up a functional cybersecurity program more rapidly and logically than would be possible without this or similar guidance

These Guidance Notes are organized as best practices and recommendations for each of the Capabilities shown in the preceding cybersecurity program graphics. The Basic Capability list deemed to be essential to a nascent program is provided first, followed by the Developed Capability list.

4.1 Basic Capability

1. Exercise Best Practices
2. Build the Security Organization
3. Provision for Employee Awareness and Training
4. Perform Risk Assessment
5. Provide Perimeter Defense
6. Prepare for Incident Response and Recovery
7. Provide Physical Security
8. Execute Access Management
9. Maintain Asset Management

4.2 Developed Capability

10. Perform Policy Management
11. Provide Standards and Governance
12. Provide and Guide Cybersecurity Hygiene
13. Gather and Use Threat Intelligence
14. Perform Vulnerability Assessment
15. Perform Risk Management
16. Provide Data Protection
17. Protect Operational Technology (OT)
18. Perform System and Security Continuous Monitoring (SCM)
19. Plan for Disaster Recovery (DR)
20. Provide Unified Identity Management
21. Perform System, Software and Application Test
22. Perform System and Application Patch and Configuration Management
23. Execute Change Control as an Enterprise Process

4.3 Integrated Capability

24. Execute Capital Planning and Investment Control
25. Implement Architecture Management
26. Provide Secure Engineering
27. Exercise Penetration Testing
28. Build Forensic Analysis
29. Enforce Privacy Data Management
30. Provide Mobile Data Management
31. Provide Certificate Management
32. Exercise Communications Management
33. Enforce Network Access Control
34. Enforce Third Party Access Management
35. Implement Secure Software Development
36. Execute Security Test & Evaluation
37. Provide and Use Audit

Each Capability section contains a series of identified recommendations and best practices that minimally satisfy the Capability, a short discussion of the section, and a list of references that are useful for further reading and understanding. The Best Practices then flow forward into the capability implementation specifications in the ABS *Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafety™ Volume 2*.

The Best Practices are set off from explanatory text and references by use of italic font to highlight the practices.

SECTION 3 Best Practices and the Application of Cybersecurity Principles to Marine and Offshore Operations: Basic Capability Set

1 Exercise Best Practices

a) *The organization maintains relationships with information sharing communities and threat or vulnerability broadcasts from both governmental and industry sources.*

b) *The organization shares threat information with peers in its community, including technical information such as indicators of compromise (IoC), to promote greater awareness and community resistance to attacks.*

c) *The organization uses regional and national resources (e.g., US-CERT, ICS-CERT and ENISA) to gain access to recent vulnerability and threat information relevant to its assets.*

d) *The organization builds a series of cultural practices that include cybersecurity requirements, thereby promoting due care and due diligence continue on a routine basis.*

e) *The organization actively engages, trains and informs its Board of Directors, or similar leadership structures and personnel, on cybersecurity practices, potential impacts of cybersecurity risks, and ongoing issues due to cybersecurity in the organization's environment and context.*

Every Company potentially benefits from involvement in the larger community. With respect to cybersecurity this is true because information exchanges, threat warnings, and best practices flow to some extent through Information Sharing and Analysis Centers (ISACs), cybersecurity professional societies, and community common interest groups. The Department of Homeland Security, federal and local law enforcement, and local or regional government agencies communicate valuable lessons learned or pertinent information briefs, and Cybersecurity Emergency Response Teams (CERTs) provide a wide variety of instructional and threat warning information notifications.

Each Company seeking to establish or maintain a cybersecurity program must make the collective decision to use the information, lessons, and accumulated wisdom gained from others in support of an internal commitment to continuous improvement. Threats do not stagnate. Threats mutate, evolve, and re-form based on changes in technology, financial gain incentives, and political agendas. Companies and security programs seeking to be unaffected by threats must not stagnate either.

The organization's leadership must be actively involved and informed with security matters, as well, so that they understand the actions required to safeguard people, assets and networks. Education for leadership and management encourages them to participate in civic and community efforts that help to inform them on topics of risk, controls and measures.

1.1 References

i) United States Computer Emergency Readiness Team (US-CERT), https://www.us-cert.gov/security-publications

ii) European Union Agency for Network and Information Security (ENISA), https://www.enisa.europa.eu/

iii) United States National Institute of Standards and Technology (NIST), *Information Security Handbook: A Guide for Managers, SP 800-100*, Oct 2006. http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

iv) United States Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT), https://ics-cert.us-cert.gov/

2 Build the Security Organization

a) *The organization matches tasks to required skills, building employee skill for long-term development of experience and institutional knowledge.*

b) *The organization performs periodic capability assessments to confirm that organizational leadership understands current security status, personnel and organizational capabilities, and gaps in processes, staffing or systems.*

Understanding one's own Company, environment, and context requires a full understanding of the organization's people, their abilities, and their skills. General rules for success include matching employees to assignments that best match the employee's interests and skills with the Company's needs as defined by its existing and road-mapped capability needs. This matching includes providing coverage for the skill sets required for security systems, applications, and appliances; for security contract management; and, for system output analysis and use. It also should also consider a look forward for employees and their skills by anticipating the changes in threat and risk environments, skills needed in the future, and career development enhancers that keep security personnel fresh, interested, and intellectually stimulated.

An important part of building the organization and the personnel is placing of expectations. Capability assessments for the Company, with status reports and plans for development, help keep personnel involved as the organization builds capabilities and matures.

2.1 References

i) United States National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE), http://csrc.nist.gov/nice/

ii) European Union Agency for Network and Information Security (ENISA), *Training Material for SMEs*, https://www.enisa.europa.eu/publications/archive/training-material-SMEs

iii) Health Information Trust Alliance (HITRUST), "Building an Information Security Organization," https://hitrustalliance.net/content/uploads/2014/03/Building-an-Information-Security-Organization.pdf

iv) United States National Institute of Standards and Technology (NIST), *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, SP 800-84*, Sep 2006. http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf

3 Provision for Employee Awareness and Training

a) *The organization has an acceptable use policy that spells out to relevant personnel the permitted uses for information technology, operational technology, and organizational data and assets.*

b) *The organization has enforcement mechanisms in place to confirm that acceptable use policies are trained, acknowledged, monitored and enforced throughout the enterprise.*

c) *The organization conducts periodic cybersecurity awareness training so that all personnel understand organizational policies, procedures, and safeguards needed to minimize threats.*

User (employee, contractor, consultant, or visitor) training for anyone who accesses Company assets is essential in order to enable employees to handle threats and risks, contemplated and unforeseen. Initial and refresher training programs that periodically review the in-place cybersecurity policies and prescriptions or proscriptions are critical for employees and contractors.

The mechanics of this training should be considered as well. Many training systems require particular provisioning or licensing on end-user machines. This can be an impediment or disincentive for occasional users (e.g., outside contractors) to access or use the training.

3.1 References

i) United States National Institute of Standards and Technology (NIST), *Building an Information Technology Security Awareness and Training Program, SP 800-50*, Oct 2003. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

ii) United States National Institute of Standards and Technology (NIST), *Information Security Handbook: A Guide for Managers, SP 800-100*, Oct 2006. http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

iii) European Union Agency for Network and Information Security (ENISA), "EU-U.S. Event on Intermediaries in Cybersecurity Awareness Raising," Jun 2012. https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/eu-u.s.-event-on-intermediaries-in-cybersecurity-awareness-raising/eu-us-event-on-intermediaries-in-cyber-security-awareness-raising

4 Perform Risk Assessment

a) *The organization performs periodic risk assessments that promote revisit to operating assumptions regarding capabilities and systems monitoring needs.*

b) *The organization exercises due care and due diligence concerning cybersecurity assets, risks, and protective systems, provisioning appropriate capabilities that yield protections which can be judged adequate against expected threats.*

c) *The organization uses a construct, or a framework, to frame the methods and techniques required to bring all cybersecurity actions, automated systems, and risk management processes into a single management system.*

d) *Risk management processes include risk indicators that allow effective and proactive handling of risks in decision making.*

Essential to any technology-dependent Company is its risk assessment process, which is in turn a critical component for decision making, and it serves as an input to the risk management process (below).

Given the current threat environment, risk assessment requires a full understanding of the characteristics, locations, and integration interfaces of assets that must be protected. Threats can include natural disasters, equipment failures, personnel failures and errors, malfeasance, external human errors, and malevolent actions, among others. Risk assessment, as a process, considers the factors that can affect its technology, its business processes, its business purpose, and its environment outside the Company. The risk assessment works to identify those factors that must be considered for risk reduction, mitigation, transfer, or acceptance. This is a formal, consciously managed process that must include the support of leadership and management by requiring and confirming that proper care is exercised during the assessment and resulting documentation of results.

4.1 References *(1 September 2016)*

i) United States National Institute of Standards and Technology (NIST), *Guide for Conducting Risk Assessments, Special Publication (SP) 800-30 Rev.1*, Sep 2012. http://dx.doi.org/10.6028/NIST.SP.800-30r1

ii) European Union Agency for Network and Information Security (ENISA), *Risk Management Process*, https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process

iii) American Bureau of Shipping, *Guidance Notes on Risk Assessment Applications for the Marine and Offshore Oil and Gas Industries*, 2000. http://ww2.eagle.org/en/rules-and-resources/rules-and-guides.html#/content/dam/eagle/rules-and-guides/current/other/97_riskassessapplmarineandoffshoreoandg

iv) International Standards Organization (ISO), *ISO/IEC 27001 – Information Security Management*, 2013, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

v) International Standards Organization, *ISO 31010 – Risk Management – Risk Assessment Techniques*, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

5 Provide Perimeter Defense

a) *The organization understands its networked systems and decides on protective systems based on the functions they provide, rather than the category or brand name. The functions integrate within the security organization to provide more complete knowledge of operational security.*

b) *Tools are effective when they are used by experienced, trained personnel who have the access and insight to interpret the tools' output as required actions.*

c) *The organization screens communications paths and messaging (e.g., email or social messaging methods) prior to its delivery into the organization, or to the recipient's mailbox, to detect and remove any hazardous files, attachments, or links.*

d) *The organization protects perimeter or protective equipment, appliances or systems against unauthorized access by use of screening mechanisms, access control lists, complex passwords and/or two-factor authentication, and out-of-band communications paths.*

e) *The organization documents and tracks security device, appliance, and system configurations and settings, for better understanding of current configurations, periodic training for existing and new personnel, and audit capability for the equipment and systems.*

Building on the previous capabilities, providing perimeter defense is not a single or simple undertaking. It requires an understanding of the networked environments and assets, the personnel and their skills and abilities, and the relative risk to assets and personnel from existing or anticipated threats.

Security architecture components must also be protected from unauthorized access, in much the same way that those security systems protect the Company's critical data, servers, and endpoints. Just as a company would not allow unfettered or concealed access to its physical site fence line and equipment parking areas, it should also prescribe conscious procedures for access to security systems, applications, appliances, and data.

5.1 References

i) United States National Institute of Standards and Technology (NIST), *Systems Security Engineering, SP 800-160*, Draft, May 2014.
http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

ii) United States National Institute of Standards and Technology (NIST), *Guide to Intrusion Detection and Prevention Systems, SP 800-94 Rev 1*, Draft, Jul 2012.
http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf

iii) United States National Institute of Standards and Technology (NIST), *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, SP 800-171*, Jun 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

iv) United States National Institute of Standards and Technology (NIST), *Guide to Secure Web Services, SP 800-95*, Aug 2007.
http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

v) United States National Institute of Standards and Technology (NIST), *Guide to Malware Incident Prevention and Handling for Desktops and Laptops, SP 800-83 Rev 1*, Jul 2013.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

vi) United States National Institute of Standards and Technology (NIST), *Guidelines on Securing Public Web Servers, SP 800-44 Version 2*, Sep 2007.
http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

vii) United States National Institute of Standards and Technology (NIST), *Guidelines on Electronic Mail Security, SP 800-45 Version 2*, Feb 2007.
http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf

viii) United States National Institute of Standards and Technology (NIST), *Guidelines on Firewalls and Firewall Policy, SP 800-41 Rev 1*, Sep 2009.
http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

6 Prepare for Incident Response and Recovery

a) *The organization has an Incident Response Plan (IRP) that incorporates:*

- *Lessons learned from previous episodes and events;*
- *Notification lists for those personnel needed to understand the incident, or to take part in the response to it;*
- *Communications plan for internal personnel that provides continued operations while dispelling fear;*
- *Communications plan for external agencies and personnel to maintain the organizational perspective;*
- *Control plan for hazards that may affect personnel or systems;*
- *Control plan for hazards that may spill from the Company's boundaries into the surrounding environment (i.e., affect neighbors or otherwise foment liability); and*
- *Recovery plan for establishing a known set of conditions, consolidating those conditions for safety of personnel, systems, ship/platform/facility, and environment, and moving back to full operational capabilities.*

b) *The organization conducts periodic and cyber incident drills that rehearse actions and reactions employed to recognize, control, and recover from a cybersecurity event that affects critical systems, data, and functions.*

The company or agency can plan for how to control and recover from threats based on its knowledge of the Company structure, employee capabilities, the Company's remediation capabilities, its current risk position and threats, and its deployed boundary defenses. It is vital that this be a collaborative, inclusive activity that involves all parties concerned with operations and operational characteristics of the company. Lessons learned from one's own efforts, and from experiences of others, are important multipliers for achieving better, faster results. The communications plans for both internal and external personnel and contacts are worked out in advance so as to avoid on-the-fly decisions, mistakes, and omissions when pressured by crisis conditions. Crisis control plans must target safety for personnel and systems, protect against environmental or surrounding organizational harms, and provide a basis for reporting to compliance organizations.

6.1 References

i) European Union Agency for Network and Information Security (ENISA), *Good Practice Guide for Incident Management*.
https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management/at_download/fullReport

ii) United States National Institute of Standards and Technology (NIST), *Computer Security Incident Handling Guide, SP 800-61 Rev 2*, Aug 2012.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

iii) United States National Cybersecurity Center of Excellence (NCCoE), "Data Integrity: Reducing the Impact of an Attack," Draft, 23 Nov 2015.
https://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_Data_Integrity_Project_Description.pdf

iv) United States National Institute of Standards and Technology (NIST), *Guide to Integrating Forensic Techniques Into Incident Response, SP 800-86*, Aug 2006.
http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

7 Provide Physical Security

a) *The organization provides security and securing methods for all computational equipment that controls aspects of safety-related operations, or interfaces to systems that control aspects of safety-related operations.*

b) *The organization keeps physical security sensor feeds and system connections logically separate from production network content, segregating physical security system data flows to prevent either casual snooping or inadvertent interference within the normal scope of network operations.*

c) *The organization confirms all computationally-enabled physical security equipment (cameras, sensors, electronic locks, networked accesses, etc.) have passwords that are (1) changed from default; and (2) non-trivial and cryptologically strong.*

d) *The organization has considered risks associated with computationally-enabled physical security equipment so that inadvertent login failures and/or lockouts, loss of power, reboot events, and the like will not impact safety-critical operations.*

e) *The organization safeguards its systems and device infrastructure with physical security and other means to limit access to critical equipment or safety-related equipment to authorized personnel, with appropriate accesses and means, only.*

f) *The organization regularly tests physical and environmental control and security sensors, devices, systems, appliances and applications, in accordance with both manufacturer and owner direction or guidance, to keep these systems in peak, known operational states.*

Physical security for marine ships and platforms is a well-established area, but the addition of information technology (IT) and operational technology (OT) systems can change the needs in unexpected ways. Owners and operators must keep in mind that cyber-enabled safety and security equipment can be attacked and suborned/disabled, as can other IT and OT systems. Data systems, computational equipment, and data storage must be safeguarded from all but authorized access, no matter the location, and safeguards must include physical blocking/locking devices and appliances, as well as spaces for such equipment and systems.

7.1 References

i) Cisco: "Network Security Policy: Best Practices White Paper," Oct 2005. http://www.cisco.com/c/en/us/support/docs/availability/high-availability/13601-secpol.html

ii) Kane, Douglas R. and Paul Viollis, checklists adapted from *Silent Safety: Best Practices for Protecting the Affluent*, American Institute of CPAs (AICPA). http://www.aicpa.org/publications/personalfinancialplanning/downloadabledocuments/checklist_operational%20security.pdf

iii) United States Department of Transportation, Maritime Administration. *Maritime Security for Vessel Personnel with Specific Security Duties, Model Course MTSA 04-01*, Dec 2004. http://www.marad.dot.gov/wp-content/uploads/pdf/MTSA_VPSSD_MODEL_COURSE_MTSA_04-01.pdf

iv) International Maritime Organization (IMO). *Guide to Maritime Security and the ISPS Code, 2012 Edition.* http://www.imo.org/en/Publications/Documents/Newsletters%20and%20Mailers/Mailers/IA116E.pdf#search=ISPS

8 Execute Access Management

a) *The organization screens personnel for security issues prior to onboarding.*

b) *The organization allows no group login credentials, and shared credentials/sharing of credentials are prohibited.*

c) *The organization requires two-factor authentication to access sensitive resources or assets, or to access networked assets remotely.*

d) *The organization periodically inventories third-party access and relationships to confirm that all network and/or data access are current, required, and under governance and control.*

e) *The organization requires authorized third-party personnel with access to organizational networked systems to use two-factor authentication for connection, or strong passwords that cannot be easily guessed.*

f) *The organization has defined, and uses, a third-party supplier program, including supplier vetting prior to granting access to networked resources.*

g) *The organization requires all remote access users to pass through security and authentication systems to provide traceability of communications and tracking or logging of actions carried out remotely. No remote access can occur without strict accountability for all communications.*

h) *The organization limits privileged access accounts to those identified personnel with specific work-related needs.*

i) *The organization limits privileged accounts to specific systems and does not allow those accounts Internet access (outside access is limited to non-privileged accounts).*

j) *The organization requires login credentials for users to access guest wireless network resources, to provide usage tracking as necessary.*

k) *The organization implements login failure time-out periods to prevent password guessing.*

l) *The organization decides single sign-on (SSO) boundaries on the basis of data or application criticality, leaving certain designated applications, systems, repositories or functions outside SSO to meter access based on separate authentication for traceability and accountability.*

m) *The organization deprovisions former employees promptly so that there are no unauthorized accesses to a former employee account after changing employment.*

Every Company with assets must meter and monitor access to those assets. Access considerations include:

- Internal personnel
- External personnel
- Privileged access
- Machine-to-machine communications

The technical means of implementing these categories of access differs across Companies, communities, and industries. The main access control program concepts must remain steady, however, no matter what the technical specifics of implementation.

The final objective of access control is simple: Know when and under what circumstances any person or machine has access to every secured entity in the Company. The check on this is to ask the simple question: "Is this how things should be in order for work to be performed in a way that safeguards the Company's assets, personnel, and data?"

8.1 References

i) United States National Cybersecurity Center of Excellence (NCCoE), *Identity and Access Management for Electric Utilities, SP 1800-2, Practice Guide for Energy Sector*, Aug 2015. https://nccoe.nist.gov/projects/use_cases/idam

ii) United States National Institute of Standards and Technology (NIST), *Electronic Authentication Guideline, SP 800-63-2*, Aug 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

iii) United States National Institute of Standards and Technology (NIST), *Security of Interactive and Automated Access Management Using Secure Shell (SSH), NISTIR 7966*, Oct 2015. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7966.pdf

iv) European Union Agency for Network and Information Security (ENISA), "EU Cybersecurity Agency Argues That Better Protection of SCADA Systems is Needed," https://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-argues-that-better-protection-of-scada-systems-is-needed

v) United States National Institute of Standards and Technology (NIST), *Guide to Enterprise Telework and Remote Access Security, SP 800-46 Rev 1*, Jun 2009. http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf

9 Ensure Asset Management

a) *The Company tracks its working technology assets and data as the critical enablers of the business or mission, protecting them logically as well as physically, to prevent unauthorized disclosures or losses.*

b) *The Company identifies and tracks critical infrastructure, both in physical assets and in functions, which require protection to safeguard the business or mission.*

c) *The Company requires authorized third-party personnel and their systems to be vetted, screened, and authorized prior to connection to the Company's networked systems.*

d) *The Company tracks and manages the obsolescent equipment and related software in operational systems, keeping awareness of vulnerabilities and exposures to communications paths that could allow unauthorized access to those assets.*

e) *The Company actively manages open resources such as guest wireless networks, requiring passwords for authorized users, system tracking (by address and/or port), and standards for acceptable use.*

Assets include data, physical property, facilities, systems, software applications, and operational capabilities or business/mission functions. Asset management addresses physical assets first, followed by logical assets (data and applications). However, the critical functions of the organization, and its abilities to execute its business-critical or mission-critical functions, must be safe from risks and threats as well.

Asset management also includes linkages to configuration and change management, vulnerability and patch management, and overall risk management. Close control of assets is more than an accounting requirement; it is also critical to understanding and controlling risk within the Company.

9.1 References

i) United States National Cybersecurity Center of Excellence (NCCoE), *IT Asset Management, SP 1800-5, Practice Guide for Financial Services*, Oct 2015. https://nccoe.nist.gov/projects/use_cases/financial_services_sector/it_asset_management

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

10 Perform Policy Management

a) *The organization tailors security policies to its specific context, environment, and compliance needs, to satisfy useful purpose as well as meeting regulatory and reporting needs.*

b) *The organization's policies and procedures align with its chosen standards (See Subsection 11 below) for policy positions that directly support organizational goals for technology, use, and enforcement.*

c) *The organization confirms that its personnel initially train on policies upon starting a new position, and that they review the enterprise policies on an assigned and regular basis.*

Policy development, application, enforcement, and monitoring activities include administrative, managerial, operational, and technical controls. Policy management may be mostly human activities to generate and promulgate policies, but as much effort and thought must be applied to application, enforcement, and monitoring of the policies and procedures. Measures and metrics, with technical means, must be devised and applied with policies so that those policies can be enforced as required. This is especially important when compliance regimes require monitoring and periodic reports for status and condition.

10.1 References

i) Hostland, Kenneth et.al. *Information Security Policy: Best Practice Document.* GEANT and UNINETT document GN3-NA3-T4-UFS126, Oct 2010. http://services.geant.net/cbp/Knowledge_Base/Security/Documents/gn3-na3-t4-ufs126.pdf

11 Provide Standards and Governance

a) *Cyber issues are covered by the governing body (Board of Directors, Executive Board, etc.) to focus on risks to the organization, investments required to address those risks, and personnel and staffing needed for solid programs.*

b) *Cybersecurity information provided to the Board is of sufficient quantity and frequency to enable solid Board understanding of cybersecurity risks in the enterprise, necessary mitigation efforts, and tradeoff decisions about those risks.*

c) *The organization has an appointed and empowered Chief Information Security Officer (CISO) (or equivalent) whose responsibilities unify all information technology, information systems and data systems security in a single point of accountability.*

d) *The CISO's reporting structure is short and direct, giving priority to enterprise risk management and risk mitigation efforts.*

e) *The organization has a governance structure that makes timely decisions about cybersecurity, systems and risk, balancing investments, business rules, and operations in order to minimize possible risks and maximize benefits from expenditures.*

Security governance must be conscious part of business enablement. As such, it is an investment interest area, a risk reporting area, and a functional (or extra-functional) component of the business, mission or organization. The standards and expectations for security, and the executive leadership's understanding and degree of risk acceptance, will determine how security is managed and executed throughout the enterprise. Industry shows that direct responsibility lines and accountability for outcomes are extremely important to gaining successful security results. Training is often required so that governing bodies, executives and technology management and/or security personnel are all synchronized in their requirements and understanding of the issues.

11.1 References

i) United States National Institute of Standards and Technology (NIST), *Performance Measurement Guide for Information Security, SP 800-55 Rev 1*, Jul 2008. http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

ii) United States National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53 Rev 4*, Apr 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

iii) United States National Institute of Standards and Technology (NIST), *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, SP 800-53A Rev 4*, Dec 2014. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

iv) United States National Institute of Standards and Technology (NIST), *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), SP 800-27 Rev A*, Jun 2004. http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

v) United States National Institute of Standards and Technology (NIST), *Guide for Developing Security Plans for Federal Information Systems, SP 800-18*, Feb 2006. http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

vi) International Standards Organization, *ISO/IEC 27001 – Information Security Management*, 2013, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

vii) International Standards Organization, *ISO 31000 – Risk Management*, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

12 Provide and Guide Cybersecurity Hygiene

a) *The organization has a security strategy that directly influences and guides the technology strategy, in consonance with business or mission requirements. The security and technology strategies then inform the technology and user communities as to how they can expect to use technology to satisfy their expected duties.*

b) *The organization does not allow default access methods, default passwords, or default system access roles to remain on operational systems once installed and configured.*

c) *The organization provides, through its acceptable use policy and periodic cybersecurity training, the user tips and methods necessary to maintain a well-functioning technology foundation, with rules and requirements made clear for the user community.*

d) *System maintainers have setup and configuration checklists, system test routines, and 'checkup' lists to help them assist users in keeping the technology environment safe and secure.*

Security hygiene is an important part of any technology program. All system users, operators and maintainers must perform system operations, which are carried out with due care for both authorized and secure practices. Proper hygiene rules must be promulgated regularly as part of regular training, and then backed up by configuration management and change control processes. Enforcement of proper hygiene is critical to keep the cybersecurity posture at a known status.

12.1 References

i) United States Computer Emergency Readiness Team (US-CERT). https://www.us-cert.gov/security-publications

ii) European Union Agency for Network and Information Security (ENISA). https://www.enisa.europa.eu/

iii) United Sates National Institute of Standards and Technology (NIST), *Information Security Handbook: A Guide for Managers, SP 800-100*, Oct 2006. http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

13 Gather and Use Threat Intelligence *(1 September 2016)*

a) *The Company gathers and uses threat intelligence to understand threat actors in the cyber world, their motivations and attack methods, and the potential for these threat actors to attack the Company.*

b) *The Company uses threat intelligence to recognize and act on signs of an attack to improve incident response reaction times.*

c) *The Company uses threat intelligence about potential threat actors and their methods to provide additional organization and controls to data or asset repositories.*

d) *The Company maintains a threat or risk distribution list inside the organization, sharing as deeply as 'need to know' requires, and as widely as personnel awareness needs.*

This best practice spawns from best practice items *1, 2 and 3* above, but it bears specific mention because it reflects a conscious action to reach out to find threat intelligence. Whether the threat information originates from open sources or from contracted sources, it can act to adjust or modulate efforts in cybersecurity. Threat reports from others can be correlated with threat intelligence information to stimulate new perimeter system measures and reporting, for example. In this way, threat intelligence can give a Company a better foundation for management of the risks being assessed and monitored.

13.1 References

i) United States National Institute of Standards and Technology (NIST), *Guide to Cyber Threat Information Sharing, SP 800-150*, Draft, Oct 2014. http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf

ii) United States Department of Homeland Security, "Information Sharing," current. http://www.dhs.gov/topic/information-sharing http://www.dhs.gov/topic/cybersecurity-information-sharing

iii) United States National Institute of Standards and Technology (NIST), *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, SP 800-171*, Jun 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

iv) European Union Agency for Network and Information Security (ENISA), *ENISA Threat Landscape 2014*, Jan 2015. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport

14 Perform Vulnerability Assessment

a) *The organization runs periodic vulnerability scans against its systems, seeking gaps in protective coverage and in configuration of systems.*

b) *The organization considers the connections of each system with reported vulnerabilities to determine the criticality of those vulnerabilities, and the priority to be assigned for patching those systems.*

c) *The organization has a process by which recognized and discovered vulnerabilities from scans and asset assessments are fed back to the risk assessment process for prioritization and decisions on mitigation actions.*

Vulnerability assessment is an important part of understanding the Company's asset base, its current exposures to threats and risk sources, and its composite risk position. Vulnerability assessment tools may be applied generally – across network segments, for example, seeking any and all current vulnerabilities – or to more focused areas.

Focused vulnerability scans can concentrate on particular threat and risk areas, or on specific asset categories or asset types. Vulnerability assessments can be usefully informed by outside reports of attack indicators (Indicators of Compromise (IoCs) as mentioned above) or attack code signatures, and they can help an organization decide the relative priority of particular mitigation efforts. It is very important for vulnerability assessments to be integrated with the asset configuration management processes for specific findings to be mitigated or corrected.

14.1 References

i) United States National Institute of Standards and Technology (NIST), *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, SP 800-37 Rev.1*, Feb 2010.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

ii) United States National Institute of Standards and Technology (NIST), *Guide to Industrial Control Systems, SP 800-82 Rev 2*, Feb 2015.
http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_rev2_markup-copy-first-draft-to-final-draft.pdf

iii) United States National Institute of Standards and Technology (NIST), *Guide to Computer Security Log Management, SP 800-92*, Sep 2006.
http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

15 Perform Risk Management *(1 September 2016)*

a) *The organization uses a risk management method or conceptual framework to contain and contextualize all cybersecurity and related risk issues into a risk management and handling system.*

b) *The organization does not pursue "perfected" security, but rather seeks a sustainable and acceptable risk posture that is economical, feasible, and supportable.*

c) *The organization communicates information system and data risks in terms that its constituents will understand, relating to financial stability, brand reputation, and operations integrity.*

d) *The organization has defined a risk tolerance strategy, monitoring the risk indicators that support that risk tolerance strategy.*

e) *The Company leadership understands the regulatory and compliance environment that affects the Company and its operations, placing any factors which may change compliance reports in the risk register for risk management.*

f) *The Company links security controls to the compliance reporting requirements, so that reporting indicates the degree of attainable security, not simple compliance.*

g) *The Company defines risk to sufficient granularity as to allow intelligent use of risk sharing mechanisms, when the Company's cybersecurity maturity allows for the decisions that support sharing or transfer of risks.*

Risk management is a separate activity from the earlier risk assessment process, and it includes more in-depth treatment of risks across the enterprise. Risk management considers and leverages all cybersecurity capabilities in an organization, with the express objective of determining the current, understandable risk posture, with the subsequent decisions that affect risk management actions to control the stated risk factors.

Risk management considers Company-level risks, which are generally concentrated above the tactical threats and risks associated with organizational systems. The risk management construct or framework must support the broader understanding of how system- or data-level risks can potentially affect business or mission processes, the Company as a whole, and the environment, community or region. This is an important process that requires serious attention from leadership and management.

15.1 References

i) United States National Institute of Standards and Technology (NIST), *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, SP 800-37 Rev.1*, Feb 2010.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

ii) United States National Institute of Standards and Technology (NIST), *Managing Information Security Risk: Organization, Mission and Information System View, SP 800-39*, Mar 2011.
http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

iii) European Union Agency for Network and Information Security (ENISA), *Inventory of Risk Management/Risk Assessment Methods and Tools*.
https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory

iv) United States Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process*, May 2012.
http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

v) American Bureau of Shipping, *Guide for Risk Evaluations for the Classification of Marine-Related Facilities*, Pub 117, Jun 2003.
http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/117_riskevalforclassofmarinerelatedfacilities/pub117_riskeval.pdf

vi) American Bureau of Shipping, *Guide for Surveys Using Risk-Based Inspection for the Offshore Industry*, Pub 120, Dec 2003.
http://ww2.eagle.org/content/eagle/en/rules-and-resources/rules-and-guides.html#/content/dam/eagle/rules-and-guides/current/offshore/120_surveys_riskbasedinspectionoffshoreindustry

vii) International Standards Organization, ISO 31000 – Risk Management, 2009.
http://www.iso.org/iso/home/standards/iso31000.htm

16 Provide Data Protection

a) *The organization identifies sensitive data assets that require protection to safeguard the business or mission.*

b) *The organization classifies its critical data so that personnel understand what data must remain behind specific safeguards. Those data assets deemed too sensitive for unprotected systems or assets, especially mobile devices, must be included in the policies promulgated to, and enforced through, all employees.*

c) *The organization secures its communications paths through commercial providers' networks by encrypting their communications paths and data transmissions to and from critical systems and functions.*

d) *All users' systems are backed up automatically to prevent accidental or inadvertent loss of data.*

e) *The organization specifies use and control of its proprietary data in contracts with third parties who must have access to that data.*

f) *The organization defines how it will exercise external providers' services (e.g., cloud services and applications) as part of expected operations. Any external service chosen must satisfy organizational requirements for data security and safeguarding.*

g) *The organization considers data and privacy protection to be equivalent to physical security in priority and consideration for asset protection.*

h) *The organization actively protects the data paths between and among its various assets, sites or facilities, especially those geographically remote or in difficult-to-reach locations.*

Data protection includes physical safeguards around repositories, servers, endpoints, and ships/platforms/facilities; portable device data protections; data-in-motion (i.e., transmission security) protections; data-at-rest (i.e., stored data) protections; and training for Company personnel on handling of data in both logical and physical forms.

Classification of data is important to help people understand the priorities and protections accorded to data, and the relative importance associated with the data property that belongs to the company. Successful classification efforts are key to data loss prevention (DLP) efforts, which, when implemented, will change habits and culture in favor of data protection in the enterprise.

Third-party partners and customers, contractors, and consultants must be considered for security of data and assets when brought into enterprise operations. Contracts should cover data protections in language that all parties readily understand. Third parties possessing Company data necessarily include cloud providers, as well as contracts with cloud infrastructure, storage, processing, or application providers, each of which must clearly address ownership, physical storage, disposal, and status at the end of the contract period.

16.1 References

i) United States National Institute of Standards and Technology (NIST), *Information Security Handbook: A Guide for Managers, SP 800-100*, Oct 2006. http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

ii) United States National Institute of Standards and Technology (NIST), *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), SP 800-122*, Apr 2010. http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

iii) United States National Institute of Standards and Technology (NIST), *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, SP 800-171*, Jun 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

17 Protect Operational Technology (OT)

a) *The organization integrates security requirements into operational technology safety cases, so that security testing will not invalidate or adversely affect safety tests, but while also including security as a fundamental part of system and human safety considerations.*

b) *The organization restricts and filters all traffic from IT-based control systems to operational and process technology systems, so that authentication and verification of commands occurs outside the OT systems, software and appliances.*

c) *The organization uses signed copies of software updates to its systems, working only with manufacturers to obtain system updates and patches.*

d) *The organization restricts access to ordinary Internet protocols and traffic (e.g., email, FTP, etc.) from machines authorized to connect to operational technology and process control systems.*

e) *The organization uses 'optical data diodes' or similar functionalities for data transmission from critical components or systems to authenticated outside users in order to minimize potential for unauthorized outside access to those systems via data reporting mechanisms.*

f) *The organization architects protective devices between information technology networks and operational technology networks to limit traffic types, protocols, and origins, and to trace and log all traffic into the operational technology network(s).*

g) *The organization tracks and monitors the risk its production systems may present to neighboring organizations, and it communicates risks and incident management plans to those neighbors and/or community.*

h) *The organization does not allow cyber-enabled systems that control, monitor, or record data from physical security systems to reside on the same control networks as the physical security systems.*

i) *The organization has manual backup capabilities for each critical operational function in the production flow, and it trains and exercises with the manual backup capabilities on a periodic basis.*

j) *The organization does not allow emergency backup capabilities, frequently associated with maintaining safety and safe shutdown capability, to be on the same communications networks or control systems as primary operational or mission systems.*

k) *The organization cross-trains cybersecurity personnel and operational technology engineers to keep communications between the organization's engineering groups open.*

l) *The organization uses fault tree analysis methods and failure mode analysis methods to find paths that can provide avenues of attack against critical systems.*

m) *The organization conducts failure mode analyses when considering system, process, or architectural changes in its operational and production systems.*

n) *The organization models and plans against cascading failures in its operational systems that could affect other systems, neighboring organizations, or the community.*

o) *The organization defines and strictly limits the types and mechanisms for file input and output to and from operational technology networks.*

Operational and process control technologies find their places across the marine and offshore sectors and throughout all ships, platforms, and facilities. The approach to architecting, building, installing, testing, operating, monitoring, and managing operational technology networks must center on the systems engineering rigor necessary to understand the systems and their operational characteristics.

Simply integrating process control technologies with general-purpose networks can introduce potential threats and real risks into the Company's production capabilities. Interfacing dissimilar technologies presents risk. Incorporation of communications methods that are available from outside the Company's boundaries (i.e., standard TCP/IP communications protocols on Internet lines) introduces the possibility that personnel or systems external to the Company may develop and exploit communications with the process control systems. This becomes a source of organizational risk that must be known, understood, documented, managed, and monitored.

17.1 References

i) United States National Institute of Standards and Technology (NIST), *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, SP 800-37 Rev.1*, Feb 2010.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

ii) United States National Institute of Standards and Technology (NIST), *Managing Information Security Risk: Organization, Mission and Information System View, SP 800-39*, Mar 2011.

iii) United States Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process*, May 2012.
http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

iv) United States National Institute of Standards and Technology (NIST), *Guide to Industrial Control Systems (ICS) Security, SP 800-82 Rev 2*, May 2015.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

v) United States Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT).
https://ics-cert.us-cert.gov/

18 Perform System and Security Continuous Monitoring (SCM)

a) *The organization monitors its security devices and their status reporting or dashboards, monitoring for proper function and for threats and risks revealed through log and alert reports.*

b) *The organization uses outside activities for monitoring any systems that cannot be managed within the bounds of its existing capabilities and/or staffing strength.*

c) *The organization performs security monitoring throughout the network, not just at the perimeter.*

d) *The organization will monitor its guest wireless network to verify that resource is not used for illicit or unauthorized purposes, and to prevent malware from freely communicating through it.*

e) *The organization will monitor its internal wireless networks to prevent unauthorized access points that grant access to the networked systems or infrastructure.*

f) *The organization monitors performance and security of its own website(s) to maintain understanding of customer response and data security, and to prevent undetected fraudulent diversions of traffic and data.*

Security Continuous Monitoring (SCM) is the process set by which perimeter and security device outputs and alert generation displays are monitored for anomalies or exceptions that might indicate abnormal events and incidents. The monitoring may be continuous with data displays and dashboards always available; or, it may be a routine series of defined actions for periodically checking dashboards for event updates. In any event, the security devices, applications, systems, and appliances in a Company's security architecture will show events that may require incident response and recovery.

The key to implementing effective SCM is to know what 'normal' in the monitored network is for a given set of conditions or circumstances. Risk assessment, vulnerability assessment scanning, threat intelligence, and asset performance monitoring all play roles in keeping analysts and monitoring personnel informed about whether there is, or is not, something to investigate.

18.1 References *(1 September 2016)*

i) United States National Institute of Standards and Technology (NIST), *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, SP 800-137*, Sep 2011. http://dx.doi.org/10.6028/NIST.SP.800-137

ii) United States National Institute of Standards and Technology (NIST), *Guide to Computer Security Log Management, SP 800-92*, Sep 2006. http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

19 Plan for Disaster Recovery (DR)

a) *The organization defines the requirements and needs for business or mission continuity in face of threats and risk conditions, and plans against those risks so that the business can continue even through serious interference effects.*

b) *The organization plans for, and resources, disaster recovery capabilities to provide continuity of business or mission capabilities when responding to risk conditions.*

c) *The organization conducts periodic table-top exercises that allow revisit of disaster plans, initial training for new personnel, and refresher training for experienced personnel.*

d) *The organization confirms that security architecture protecting the existing systems, facilities, personnel, and assets is adequately replicated in terms of functions during a disaster recovery scenario. Under no circumstance should a DR effort leave security undone.*

Mission-critical functions are cataloged as part of asset management. As such, the technology team in the Company must have plans in place to recover from highly unusual ('black swan') events. These plans might be enabled by physical relocation, alternate equipment, alternative work regimes (i.e., working from home), or a combination of all. Disaster recovery is the largest possible case for incident response and recovery, and the effort must be planned, resourced, staffed, tested, and periodically refreshed.

19.1 References *(1 September 2016)*

i) United States National Institute of Standards and Technology (NIST), *Contingency Planning Guide for Federal Information Systems, SP 800-34 Rev 1*, May 2010. http://dx.doi.org/10.6028/NIST.SP.800-34r1

ii) European Union Agency for Network and Information Security (ENISA), "IT Continuity Home," https://www.enisa.europa.eu/activities/risk-management/current-risk/bcm-resilience

20 Provide Unified Identity Management

a) *The organization establishes and maintains consistent processes for managing identity and data access information about users, to establish who they are, to what groups they belong, how they are authenticated and what they can access among enterprise assets.*

b) *The organization provisions and supports single sign-on (SSO) methods across systems, with governance decisions made concerning assets that must require specific, separate login for access traceability.*

c) *The organization establishes identity governance processes involving all organizational stakeholders (application owners, human resources department, payroll department, IT department, and data owners) to provide accurate, timely, and auditable operational processes for user provisioning and de-provisioning.*

d) *The organization uses measures and metrics to gauge effectiveness and improvements in the various identity processes that span departments or divisions, including such areas as times to provision or de-provision access; frequency of directory cleanup sweeps; numbers of shared or group credentials; numbers of failed logins, and lockout frequency; etc. This data is useful for process improvement, and it also serves as very useful input to log examination and management.*

e) *System and data access are apportioned on the basis of user roles, job responsibilities, and role attributes, which data is maintained in the master human resources data repositories for authoritative sources.*

A unified identity means consistency across user identity-determined roles and accesses. With many Companies provisioning and supporting dozens, and potentially hundreds, of applications across their enterprises, unification of identity and access management processes becomes a supportability issue for both technology (security and operations) and human resources groups. Consistent login and data access management, supervision and audit must apply across all areas of actual or potential user contact with assets, including data assets and functional assets.

Key to unified identity is the decisions and policies to be implemented and enforced, then measured, in pursuit of effectiveness and efficiency. Companies must provide the 'single source of truth' for personnel roles, accesses, authorizations, and identities, if they are to realize efficiencies and effective capabilities for user management and access tracking.

20.1 References

i) United States National Institute of Standards and Technology (NIST), *A Comparison of Attribute Based Access Control (ABAC) Standards for Data Services, Draft, SP 800-178*, Dec 2015. http://csrc.nist.gov/publications/drafts/800-178/sp800_178_draft.pdf

ii) European Union Agency for Network and Information Security (ENISA), "Trust and Reputation Models," https://www.enisa.europa.eu/activities/identity-and-trust/library/trust-and-reputation-models

iii) United States National Institute of Standards and Technology (NIST), *Electronic Authentication Guideline, SP800-63-2*, Aug 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

21 Perform System, Software, and Application Test

a) *The organization has an authorization process for software upgrades that does not allow unexpected, unattended, or unauthorized software to be loaded in critical systems, or in operational systems that connect to critical systems.*

b) *The organization tests all software for functional and security requirements prior to making that software available to users. Any software found lacking in the test process is not installed.*

c) *The organization uses a periodic security evaluation tool and process to assess its current status, any gaps in security coverage, and outstanding requirements that may affect its overall security profile.*

d) *The organization has internal audit capabilities for cybersecurity, and those personnel understand the cybersecurity context of the organization.*

If the risk profile of the Company is to be granular and realistic, the team governing software installation must be aware of any and all software operating inside an organization. While hundreds of applications and software components may be present, the Company must have an ability to test and approve software to allow employees to carry out their duties, while simultaneously allowing the organization to manage and understand its software foundations. Testing must include both functional (what the software is supposed to do) and extra-functional (security and behavior) aspects.

In a complex organization, testing graduates from individual systems to systems of systems, and to entire network segments and network architectures. As systems, software, and applications are added to a Company's environment, the test organization must develop capabilities to examine the entirety of the hosted environment(s) to seek opportunities for improvement and security gap closure.

21.1 References *(1 September 2016)*

i) United States National Institute of Standards and Technology (NIST), *Technical Guide to Information Security Testing and Assessment, SP 800-115*, Sep 2008. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

ii) American Bureau of Shipping, *Guide for Integrated Software Quality Management (ISQM)*, Jul 2014. http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/185_isqm/ISQM_Guide_e-Feb16-New%20Logo.pdf

iii) International Standards Organization, *ISO/IEC/IEEE 29119-3:2013 – Software and Systems Engineering – Software Testing – Part 3: Test Documentation*. http://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2FIEC%2FIEEE+29119-3%3A2013

22 Perform System and Application Patch and Configuration Management

a) *The organization catalogs its hardware configurations and software holdings and licenses so that it can prioritize and apply patches that address identified vulnerabilities arising from threat reports, vulnerability scans, or risk analyses.*

b) *The organization tests system and application patches on a testbed prior to applying the patches to operational systems.*

c) *The organization understands and controls the use of applications and executable software in its systems, and it restricts any software from running unless the software has been tested and approved for use (whitelisting).*

The threat-vulnerability-configuration-patch-change-risk management cycle leverages many sides of the technology management domain to include as many considerations as possible when integrating new software, patches, or changes in system configuration when integrated with the enterprise networked systems' architectures.

System and application patch testing, whether on information technology systems, or on operational technology or process control systems, is an important consideration to reduce the risk associated with pushing new software into standing, (presumably) functioning systems, with the intent of modifying the existing, working software.

Equally important, however, is documentation of existing systems and changes to those systems. Corporate knowledge in the Company requires continuity and currency of documentation, so that personnel can learn from what they have, study it to improve operations and systems, and pass their knowledge along for the betterment of the larger organization.

22.1 References *(1 September 2016)*

i) United States National Institute of Standards and Technology (NIST), *Guide for Security-Focused Configuration Management of Information Systems, SP 800-128,* Aug 2011. http://dx.doi.org/10.6028/NIST.SP.800-128

ii) United States National Institute of Standards and Technology (NIST), *Guide to General Server Security, SP 800-123*, Jul 2008. http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

iii) United States National Institute of Standards and Technology (NIST), *Guide to Enterprise Patch Management Technologies, SP 800-40 Rev 3*, Jul 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

23 Execute Change Control as an Enterprise Process

a) *The organization has an authorization process for hardware, software, firmware, and architecture or configuration upgrades that does not allow unexpected, unattended, or unauthorized changes to be made to critical systems, or in operational systems that connect to critical systems.*

b) *A formal, rigorous change control process is critical to documenting both information technology and operational technology systems, maintaining enterprise knowledge of both, and implementing cybersecurity controls and security.*

c) *The organization maintains logs, system diagrams, and records for all business-critical or mission-critical systems that note the changes made during the change control processes.*

Change control is the process by which patches, vulnerability mitigation actions, architectural changes, system improvements, software updates, system concept of operations changes, staffing and supportability changes, and security improvements are registered and approved across the Company. Changes are then cataloged and documented to confirm completeness for accessibility and searchability within the enterprise.

23.1 References *(1 September 2016)*

i) United States National Institute of Standards and Technology (NIST), *Performance Measurement Guide for Information Security, SP 800-55 Rev 1*, Jul 2008. http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

ii) United States National Institute of Standards and Technology (NIST), *Guide for Security-Focused Configuration Management of Information Systems, SP 800-128*, Aug 2011. http://dx.doi.org/10.6028/NIST.SP.800-128

SECTION 5 Best Practices and the Application of Cybersecurity Principles to Marine and Offshore Operations: Integrated Capability Set

24 Execute Capital Planning and Investment Control (CPIC)

a) *The organization prioritizes key risk areas for investment and improvement to keep risks understood and manageable. The prioritized areas are consistent with the publicized budget goals and objectives.*

b) *The organization considers security as at least equivalent to economics when pursuing system, process, or architecture changes.*

Security must be implemented through the governance process that performs risk management efforts as part of the decisions associated with managing the Company's assets and capabilities. Therefore, security investments become part of the overall information technology and operational technology implementation, engineering, and operations strategies. As such, the internal priorities processed from strategy establishment, to portfolio management, to budget generation remain consistent with the Company's goals for security and operability in support of enterprise business functions.

24.1 References *(1 September 2016)*

i) United States National Institute of Standards and Technology (NIST), *Recommendations for Integrating Information Security into the Capital Planning and Investment Control (CPIC) Process, SP 800-65 Rev 1, Retired Draft*, Jul 2009.
http://csrc.nist.gov/publications/drafts/800-65-rev1/draft-sp800-65rev1.pdf

ii) United States Office of Management and Budget (OMB), *Management and Oversight of Federal Information Technology*,
https://management.cio.gov/

iii) United States Office of Management and Budget (OMB), *Guidance for Benefit-Cost Analysis for CPIC*.
https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2016_guidance.pdf

25 Implement Architecture Management *(1 September 2016)*

a) *The Company's security projects are under specific, accountable control for effective accomplishment and deterministic contribution to the organization's systems architecture.*

b) *The Company uses architectural and design features to limit possible intrusions and illicit movements within the organization's networked boundaries, giving additional time for detection and defeat of unauthorized access.*

c) *The Company considers traffic patterns and flow in architectural and design choices of transmission systems and protocols, and it plans for traffic capacity in choices of operational technology nodes and components.*

d) *The Company does not allow cyber-enabled systems that add capabilities to physical security systems to reside on the same control networks as the physical security systems.*

e) *The Company will not allow equipment emplaced for maintenance, prototyping, experimentation or proof-of-concept development to remain in place after the conclusion of the operation, especially if that equipment included communications connections or interfaces that were not documented as part of the main systems' architectures.*

The architecture for systems security architecture is closely coupled to architecting, designing, building, and maintaining systems and systems of systems (such as ships, platforms, facilities, vehicles, etc.) Architecture is key to preventing undesired outcomes. If potential failure modes are identified during initial design phases, those modes can be removed from the design so that they represent no threat. Similarly, human interference options in a system can be architected, designed, and overtly removed from end product functional outcomes.

Use of architecture in this way requires a focus on system assurance and operational outcomes. System engineers and builders have been known to reduce functionality on the basis of pure economics (in that one part costs less than another) or on ease of design, rather than foreseeing the desired operational end states – including acceptable security protection.

Architectural guides and restraints on design can limit future growth and flexibility if they are not carefully considered and implemented during the engineering of the system(s).

25.1 References

i) United States National Institute of Standards and Technology (NIST), *Systems Security Engineering, SP 800-160*, Second Draft, May 2016.
http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf

ii) United States National Institute of Standards and Technology (NIST), *Recommendations for Integrating Information Security into the Capital Planning and Investment Control (CPIC) Process, SP 800-65 Rev 1*, Draft, Jul 2009.
http://csrc.nist.gov/publications/drafts/800-65-rev1/draft-sp800-65rev1.pdf

26 Provide Secure Engineering *(1 September 2016)*

a) *The Company architects, designs, and builds systems and processes with monitoring and security or performance measurement in mind.*

b) *The Company installs systems on its networks with pre-defined, approved security hardening configurations that minimize the potential for unexpected vulnerabilities.*

c) *The Company secures its communications paths through commercial providers' networks by encrypting their communications paths and data transmissions to and from critical systems and functions.*

d) *The Company manages encryption methods and cryptography suites so as to remain current with industry standards, personnel skills and capabilities to manage, and supportability for chosen standards through the security architecture.*

e) *The Company designs protection between information technology networks and operational technology networks to limit traffic types, protocols and origins, and to trace and log all traffic into the operational technology network(s).*

f) *The Company installs peripherals on its networks with pre-defined, approved security hardening configurations that remove web and wireless network servers and protocols prior to connection to the network.*

g) *The Company specifically authorizes, and limits operational protocols to, those protocols needed on the network for business-critical requirements.*

h) *The Company terminates all VPNs outside the boundaries of any critical systems or components, and at nodes that are monitored for access and activity.*

i) *The Company provides protective screening and filtering of VPN-borne traffic to prevent malware on remotely-connected systems from transiting the VPN into the main networked systems without passing through a security monitoring package.*

j) *The Company uses secure maintenance methods that include limits on what computer-based maintenance assist or analysis gear can be used for, and with what systems; how systems will be patched and updated (in accordance with prior change control practices); and how maintenance personnel on cyber-enabled systems will be trained and certified to recognize signs of reportable abnormalities, anomalies and exceptions that may indicate safety and security issues.*

Secure engineering practices naturally follow architecture management in a security-aware and security-capable organization. The practices needed to execute secure engineering include aspects of engineering, operations, and maintenance to prevent undesired outcomes before they can manifest. Working with the system architects, engineers can implement processes and procedures that encourage secure operations, protect systems from unexpected input or contact, and monitor and alert on anomalous conditions. Secure engineering includes feedback to Security Continuous Monitoring processes so that measures, metrics and monitored parameters are reviewed and used for abnormal conditions and incident identification and control.

26.1 References

i) United States National Institute of Standards and Technology (NIST), *Security Considerations in the System Development Life Cycle, SP 800-64 Rev 2*, Oct 2008.
http://dx.doi.org/10.6028/NIST.SP.800-64r2

ii) United States National Institute of Standards and Technology (NIST), *Security Guide for Interconnecting Information Technology Systems, SP 800-47*, Aug 2002.
http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

iii) United States National Institute of Standards and Technology (NIST), *Systems Security Engineering, SP 800-160*, Draft, May 2014.
http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

iv) United States National Institute of Standards and Technology (NIST), *Guidelines on Securing Public Web Servers, SP 800-44 Version 2*, Sep 2007.
http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

v) United States National Institute of Standards and Technology (NIST), *Guidelines on Electronic Mail Security, SP 800-45 Version 2*, Feb 2007.
http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf

vi) United States National Institute of Standards and Technology (NIST), *Guidelines on Firewalls and Firewall Policy, SP 800-41 Rev 1*, Sep 2009.
http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

vii) United States National Institute of Standards and Technology (NIST), *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), SP 800-27 Rev A*, Jun 2004.
http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

27 Exercise Penetration Testing *(1 September 2016)*

a) *The Company uses penetration testing to determine the effectiveness of their protective systems and process controls by testing the enterprise technical systems against adversary-like methods.*

b) *The Company applies best practices for system hardening prior to penetration testing, using the test to show discrepancies and gaps, rather than expecting the test to show the entire requirement for hardening.*

c) *The Company uses penetration testing results to generate an action list that can inform the capital development plan for budgeting security improvements.*

The Company can manage and limit its system weaknesses by understanding, and testing, its exposure to outside attack. Penetration testing methods can provide visibility for unmitigated vulnerabilities; highlight specific configuration problems in endpoints, servers or infrastructure; and demonstrate where additional protective layers (either technical functions or processes) will benefit the data protection and system protection requirements.

All assets that may have exposure to human error, failure conditions, illicit insider access or outside malicious attack are to be considered for penetration testing. Testing can be accomplished in multiple phases, if needed, but that can lead to disconnects between repair needs and responsibilities for budgeting and implementing the mitigation actions. System applications, user systems (desktop, laptop and office automation systems), servers, office utilities (e.g., printers or multi-function devices), infrastructure systems, physical security systems, vehicles, and sensors, among other entities, are to be considered for testing.

27.1 References

i) United States National Institute of Standards and Technology (NIST), *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, SP 800-53A Rev 4*, Dec 2014. http://csrc.nist.gov/publications/nistpubs/800-53A-rev4/sp800_53a_r4_errata_12_18_2014.docx

ii) United States National Institute of Standards and Technology (NIST), *Mobile Application Vetting Services for Public Safety, Draft NISTIR 8136*, June 2016. http://csrc.nist.gov/publications/drafts/nistir-8136/nistir_8136_draft.pdf

iii) United States National Institute of Standards and Technology (NIST), *Systems Security Engineering, SP 800-160*, Draft, May 2014. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

iv) Software Assurance Community Resources and Information Clearinghouse, *Software Assurance Pocket Guide Series: Development, Volume VI version 2.0, May 18, 2012.* https://buildsecurityin.us-cert.gov/sites/default/files/SecureCoding_PocketGuide_v2%200_05182012_PostOnline.pdf

28 Build Forensic Analysis *(1 September 2016)*

a) *The Company builds and maintains forensic analysis skills, tools and procedures to provide technology personnel the appropriate foundation and abilities to execute forensic evidence gathering and forensic analysis, both to satisfy malware or intrusion-related forensic analysis, and to assist in Legal or HR-related investigatory activities.*

b) *The Company structures forensic activities under enterprise policy to include specifically the Legal, Human Resources and Privacy departments for their collaborative roles in forensic evidence gathering.*

c) *The Company links specific objectives under security continuous monitoring activities to forensic activities and processes, the better to preserve indicators of attack or indicators of compromise for forensic and damage analyses.*

The Company may include internal capabilities to perform forensic analysis on cybersecurity events, to complement the continuous monitoring capabilities previously deployed. Forensic evidence gathering is a specialty area that will assist with not just malware event recovery but also with data discovery in case of legal inquiries.

Forensic capabilities may be included in applications or systems built into the Company's practices or infrastructure. Software may be designed to generate forensic feedback if they are attacked, for example. All new systems provide the opportunity to insert software that senses abnormal or malicious conditions and report to the owner.

28.1 References

i) United States National Institute of Standards and Technology (NIST), *Security Considerations in the System Development Life Cycle, SP 800-64 Rev 2*, Oct 2008. http://dx.doi.org/10.6028/NIST.SP.800-64r2

ii) United States National Institute of Standards and Technology (NIST), *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, SP 800-137*, Sep 2011. http://dx.doi.org/10.6028/NIST.SP.800-137

iii) United States National Institute of Standards and Technology (NIST), *Guide to Computer Security Log Management, SP 800-92*, Sep 2006. http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

iv) United States National Institute of Standards and Technology (NIST), *Systems Security Engineering, SP 800-160*, Draft, May 2014. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

v) European Union Agency for Network and Information Security (ENISA), *Electronic Evidence: A Guide for First Responders*, 25 March 2015. https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders

vi) European Union Agency for Network and Information Security (ENISA), "ENISA's Updated Training Material in Network Forensics," 02 March 2015. https://www.enisa.europa.eu/news/enisa-news/enisas-updated-training-material-in-network-forensics

vii) European Union Agency for Network and Information Security (ENISA), *Network Forensics: Handbook, Document for Teachers*, February 2015. https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/network-forensics-handbook

29 Enforce Privacy Management *(1 September 2016)*

a) *The Company understands its legal, regulatory, policy and guidelines environment for the geographic areas or nations in which it operates, and it safeguards personnel data to the strictest standards required by the most stringent compliance requirements.*

b) *The Company segregates personnel and privacy-related data away from other, less-critical data, to reduce the potential for breaches to enterprise data including privacy-related data.*

c) *The Company vets personnel with access to privacy-related data, and it limits access to only those personnel.*

d) *The Company appoints an official with technical knowledge of networked systems to be in charge of privacy-related data and issues therein.*

Privacy is a special case of data security (Capability 16, above) due to the potential value of, or impact associated with, personnel-related data. The Company must understand the content and classification of its data, both internally for protective controls, and externally in terms of the legislative and regulatory requirements for management of privacy-related data.

Privacy data encompasses personnel records, protected health records, system usage monitoring data, personal locator data, and anything that can contribute to understanding personal behavior. The Company's appropriate use policy for its technology systems will address expectations about personnel behavior and use, but aspects of tracking, monitoring and training will apply to privacy restrictions. This is a cross-domain security integration area that requires specific attention for companies to maintain security.

29.1 References

i) United States National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53 Rev 4, Appendix J*, Apr 2013.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

ii) United States National Institute of Standards and Technology (NIST), *Guidelines on Security and Privacy in Public Cloud Computing, SP 800-144*, Dec 2011.
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

iii) United States National Institute of Standards and Technology (NIST), *Systems Security Engineering, SP 800-160*, Draft, May 2014.
http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

iv) European Union Agency for Network and Information Security (ENISA), *Information Security and Privacy Standards for SMEs*, 17 June 2016.
https://www.enisa.europa.eu/publications/standardisation-for-smes

v) European Parliament and Council of the European Union, *General Data Protection Regulation of 27 April 2016*.
http://ec.europa.eu/justice/data-protection/reform/index_en.htm

30 Provide Mobile Data Management *(1 September 2016)*

a) *The Company understands its legal, regulatory, policy and guidelines environment for the geographic areas or nations in which it operates, and it safeguards personnel and mobile data to the strictest standards required by the most stringent compliance requirements.*

b) *The Company implements a Mobile Data Management (MDM) program that can meter, monitor and control enterprise data content on mobile devices enrolled in the program.*

c) *The Company requires employees with any mobile device (phone, tablet, non-enterprise laptop, reporting sensor, etc.) to enroll in the MDM program prior to receiving enterprise data access through the device.*

d) *The Company has, promulgates and trains employees on a formal device management policy that covers correct use and access of enterprise resources by portable devices.*

The Company treats its mobile devices as extensions of its installed infrastructure, including understanding those devices' roles in both accessing Company data, and in securing that data against unauthorized access. Included in that treatment is monitoring and enforcement mechanisms for the data and access privileges from mobile devices to enterprise resources: applications, data, remote access methods, and system functions.

It is critical to manage mobile connections and access when allowing mobile devices to connect to cyber-physical systems. Many times, remote access from mobile devices is done for convenience, with no security or special authentication required. In these cases, mobile access must be restricted to require accountability, and deliberate decisions are to be made about who, how and under what conditions such access is allowed by the Company.

30.1 References

i) United States National Institute of Standards and Technology (NIST), *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security, SP 800-46 Rev 2*, Jul 2016.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

ii) United States National Institute of Standards and Technology (NIST), *User's Guide to Telework and Bring Your Own Device Security, SP 800-114 Rev 1*, Jul 2016.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf

iii) United States National Institute of Standards and Technology (NIST), *Mobile Application vetting Services for Public Safety, Draft NISTIR 8136*, Jun 2016.
http://csrc.nist.gov/publications/drafts/nistir-8136/nistir_8136_draft.pdf

iv) European Union Agency for Network and Information Security (ENISA), *Smartphones: Information Security Risks, Opportunities and Recommendations for Users*, 10 Dec 2010. https://www.enisa.europa.eu/publications/smartphones-information-security-risks-opportunities-and-recommendations-for-users

31 Provide Certificate Management *(1 September 2016)*

a) *The Company uses cryptographic certificates to authenticate personnel, systems, messaging, portable devices, sensors and other enterprise systems to provide accountable, reliable and integrity-enhancing methods for granting access to enterprise systems and data.*

b) *The Company manages cryptographic certificates across the enterprise with a management system that matches personnel, devices, certificates, issue and expiry dates, certificate originator, and other data as required.*

The Company may assign certificates for use with personnel, portable devices, desktop computers, servers, major applications, web servers, and any other enterprise systems that can accept certificates and encryption. Certificates provide for traffic encryption, transaction or activity privacy, and authentication by integrity-enhancing means.

Certificates may multiply in use, and they require care and attention in order that they are managed appropriately. User endpoints (i.e., desktop machines, laptops, or tablets) may accumulate multiple certificates each if they are not periodically checked for current certificates and expiration dates. Similarly, servers, whether internal or external-facing, may use certificates to provide encryption in traffic streams, as well as user authentication for services. If those certificates expire without appropriate server-side actions, the provided services may be rendered insecure, leaving a gap into the enterprise networks.

31.1 References

i) United States National Institute of Standards and Technology (NIST), *Recommendation for Key Management, Part 1, SP 800-57 Rev 4*, Jan 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

ii) United States National Institute of Standards and Technology (NIST), *Electronic Authentication Guideline, SP 800-63-2*, Aug 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

iii) United States National Institute of Standards and Technology (NIST), *Best Practices for Privileged User PIV Authentication, white paper*, 21 Apr 2016. http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf

iv) European Union Agency for Network and Information Security (ENISA), *Qualified Website Authentication Certificates*, 16 May 2016. https://www.enisa.europa.eu/publications/qualified-website-authentication-certificates

32 Exercise Communications Management *(1 September 2016)*

a) *The Company limits its total connections to the Internet to planned, finite numbers that can be easily managed, accounted, and audited, and each of which can be screened through security appliances and systems.*

b) *The Company secures its communications paths through contract terms with providers to maintain reliability and security of communications functions.*

c) *The Company will run periodic inventories against its contracts and technical architecture, verifying its external connections to the Internet and to other transmission paths.*

d) *The Company verifies its communications paths between and among assets, systems and facilities support data protection methods (i.e., encryption) and technical performance auditing and monitoring.*

The Company can manage and limit its exposure to outside attack by consciously limiting the number of communication lines connecting the Company to the Internet. Each and every communication line must be screened with protective devices to provide the best coverage in Security Continuous Monitoring, and to protect users and systems from outside hazards. Contracts with providers can help with safeguards on traffic (data-in-motion encryption), transmission terminal points ('last mile'), and secure connections to cloud application providers.

On-shore and off-shore communication paths among assets and facilities must be able to be monitored and audited. These paths, often within the logical boundaries of a Company's networking infrastructure, may penetrate other organizations' thresholds while in the communications lines and thereby present a risk. These paths must be considered for relative risk of intercept, the value and types of data (classification) carried to and from the remote locations, and performance measures that can indicate problems in the communication system itself.

32.1 References

i) United States National Institute of Standards and Technology (NIST), *Security Considerations in the System Development Life Cycle, SP 800-64 Rev 2*, Oct 2008. http://dx.doi.org/10.6028/NIST.SP.800-64r2

ii) United States National Institute of Standards and Technology (NIST), *Security Guide for Interconnecting Information Technology Systems, SP 800-47*, Aug 2002. http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

iii) United States National Institute of Standards and Technology (NIST), *Systems Security Engineering, SP 800-160*, Draft, May 2014. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

33 Enforce Network Access Control *(1 September 2016)*

a) *The Company restricts endpoint or device access based on authenticated entry and device or system compliance with the enterprise security policy.*

b) *The Company uses network access control as a means to direct personnel or systems to the network resources to which they have been granted access by their roles or identity attributes.*

The Company can manage and limit its exposure to unauthorized network presence by use of technical network access control (NAC) methods and user authentication certificates. As Companies grow larger, it becomes more important for employees' roles and responsibilities – and attendant areas of work – to be codified with greater definition. NAC methods can provide access to specific resources, or logical areas within a network environment, to reduce possibilities for unauthorized data access, unauthorized system access, or unauthorized presence around operational resources. NAC is an integrated implementation capability which requires technical and process controls from user authentication and identification, human resources management, and network technical access areas.

33.1 References

i) United States National Institute of Standards and Technology (NIST), *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security, SP 800-46 Rev 2*, Jul 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

ii) United States National Institute of Standards and Technology (NIST), *User's Guide to Telework and Bring Your Own Device Security, SP 800-114 Rev 1*, Jul 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf

iii) United States National Institute of Standards and Technology (NIST), *Attribute Metadata, Draft Internal Report, NISTIR 8112*, Aug 2016. http://csrc.nist.gov/publications/drafts/nistir-8136/nistir_8136_draft.pdf

iv) United States National Institute of Standards and Technology (NIST), *Guide to Attribute Based Access Control (ABAC) Definition and Considerations, SP 800-162*, Jan 2014. http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

34 Enforce Third Party Access Management *(1 September 2016)*

a) *The Company takes precautions for third party (outside) access to enterprise resources in order to establish evidence-based trust and systemic monitoring to verify ongoing trust as the third party is granted access to data and systems.*

b) *The Company performs due diligence audits, or uses professional auditors' reports, on the third party vendors, suppliers, or contractors to whom they will grant access to enterprise data, systems and network resources.*

c) *The Company confirms access to systems, data and network resources is addressed in contracts between the parties.*

d) *The Company confirms access to systems, data and network resources is both monitorable and actively monitored for anomalous behaviors and exceptions to policy.*

Third parties have legitimate reasons to access Company resources, when a relationship exists between the organizations. Third parties may include contractors or consultants; suppliers; maintenance personnel; logistic support personnel; or others who work with or for the Company. When third parties are properly vetted and contracted, certain expectations must be in place on both sides of the contract or service level agreement, thereby providing security and understanding to Company personnel and to the third parties.

The Company is interested in safeguarding its own data, systems, personnel and system functions. Toward that end, the Company must vet third parties who will have access to Company systems or data; check and approve the methods by which third parties access, use systems and data, and how they store Company data; and how authentication methods will allow third party access with surety in identification and location. It is critical to the Company that contractors and third parties do not introduce exploitable vulnerabilities into the Company via systems or personnel not under Company control.

34.1 References

i) United States National Institute of Standards and Technology (NIST), *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security, SP 800-46 Rev 2*, Jul 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

ii) United States National Institute of Standards and Technology (NIST), *User's Guide to Telework and Bring Your Own Device Security, SP 800-114 Rev 1*, Jul 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf

iii) United States National Institute of Standards and Technology (NIST), *Systems Security Engineering, SP 800-160*, Draft, May 2014. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

iv) United States National Institute of Standards and Technology (NIST), *Attribute Metadata, Draft Internal Report, NISTIR 8112*, Aug 2016. http://csrc.nist.gov/publications/drafts/nistir-8136/nistir_8136_draft.pdf

v) United States National Institute of Standards and Technology (NIST), *Guide to Attribute Based Access Control (ABAC) Definition and Considerations, SP 800-162*, Jan 2014. http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

vi) United States National Institute of Standards and Technology (NIST), *Best Practices in Supply Chain Risk Management, Conference Materials*, 14 Jun 2016. http://csrc.nist.gov/scrm/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

vii) United States National Institute of Standards and Technology (NIST), *Supply Chain Risk Management Practices for Federal Information Systems and Organizations, SP 800-161*, Apr 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

viii) United States National Institute of Standards and Technology (NIST), *Protecting Controlled Unclassified Information in Nonfederal Information Systems, SP 800-171*, Jun 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

35 Implement Secure Software Development *(1 September 2016)*

a) *The Company requires its development organizations to use secure software development techniques and methods when generating software or firmware for any system, application or device in the enterprise.*

b) *The Company uses technical software testing methods and techniques to verify its software meets enterprise and/or external customer compliance requirements.*

c) *The Company introduces security requirements and constraints into the development process as early as practicable, ensuring the security and engineering or development teams work together to reduce and remove software risks to the Company.*

d) *The Company standardizes and requires usage of enterprise security services to be used across all possible applications and systems, including such functions as network authentication, authorization for access, federated authentication for third parties, and network access via virtual private network (VPN).*

e) *The Company safeguards software code as Intellectual Property (IP) to provide appropriate protection against loss or theft on a par with physical property safeguards.*

f) *The Company confirms that development is conducted in supportable, modern languages, in modules or partitions that enable useful technical reviews and code walkthroughs.*

The Company's assets are increasingly software-intensive systems. Both internal systems and vendor-supplied systems reside on Company networks; as such, the Company requires understanding that the software in its systems has been built to standards that support safety and security.

Software must be testable and tested in order to demonstrate trustworthiness and predictability needed in safety-critical or mission-critical systems onboard ships, on-shore facilities and at-sea assets. That means the software must be designed, coded and built to secure development standards, supportable through coding deployment, and the in-the-field life cycle. Development methodologies may require some adjustments to incorporate extra-functional requirements (i.e., security) and additional test cases to support security integration during deployment. Third party suppliers of code and automated systems may require additional guidance from the Company for expectations on code security.

35.1 References

i) United States National Institute of Standards and Technology (NIST), *Security Considerations in the System Development Life Cycle, SP 800-64 Rev 2*, Oct 2008. http://dx.doi.org/10.6028/NIST.SP.800-64r2

ii) United States National Institute of Standards and Technology (NIST), *Security Guide for Interconnecting Information Technology Systems, SP 800-47*, Aug 2002. http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

iii) United States National Institute of Standards and Technology (NIST), *Systems Security Engineering, SP 800-160*, Draft, May 2014. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

iv) United States National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53 Rev 4*, Apr 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

v) Software Assurance Forum for Excellence in Code (SAFECode), *Principles for Software Assurance Assessment*, 2015. https://www.safecode.org/publication/SAFECode_Principles_for_Software_Assurance_Assessment.pdf

vi) Software Assurance Forum for Excellence in Code (SAFECode), *Fundamental Practices for Secure Software Development, 2nd Ed.*, 8 Feb 2011. https://www.safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf

vii) United States Cybersecurity Emergency Response Team (US-CERT) Software and Supply Chain Assurance Community Resources and Information Clearinghouse (CRIC), *Software Assurance Pocket Guide Series*, 2012.
https://buildsecurityin.us-cert.gov/swa/software-assurance-pocket-guide-series

viii) Open Web Application Security Project (OWASP), *OWASP Top 10 Proactive Security Controls 2016.*
https://www.owasp.org/images/5/57/OWASP_Proactive_Controls_2.pdf

36 Execute Security Test and Evaluation *(1 September 2016)*

a) *The Company uses Security Test and Evaluation (ST&E) for all software applications and development projects, ensuring build and/or installation meet enterprise security requirements.*

b) *The Company uses ST&E to identify and mitigate enterprise risk conditions or challenges,*

c) *The Company maintains and uses a security test bed for all ST&E activities, providing a representative environment for testing of software prior to deployment to operational ships, platforms, assets or facilities.*

d) *The Company uses ST&E test resources as an enterprise asset, documenting and maintaining the asset set as any other enterprise asset would require for configuration control, system training, periodic maintenance and upkeep, etc.*

The Company uses security test and evaluation (ST&E) for all cyber-enabled and software-intensive systems in order to reduce risk, prove dependability and trustworthiness, and to identify and remove flaws in systems and coding that may cause cascading failures across systems.

ST&E is important for internal systems and software, in order to understand functional soundness and interoperability, but also for packaged or third-party software. All software systems with exposure to networks (and, by extension, to the Internet in many cases) must be tested to identify potential vulnerabilities to unknown outside agents. ST&E can also reveal functional design flaws in internal software that may cause risk conditions if the flaws are allowed to persist – or not found, can reveal if the Company does not provide adequate resources for security testing.

36.1 References

i) United States National Institute of Standards and Technology (NIST), *Supply Chain Risk Management References.*
http://csrc.nist.gov/scrm/references.html

ii) United States National Institute of Standards and Technology (NIST), *Security Considerations in the System Development Life Cycle, SP 800-64 Rev 2*, Oct 2008.
http://dx.doi.org/10.6028/NIST.SP.800-64r2

iii) Open Web Application Security Project (OWASP).
https://www.owasp.org/index.php/Main_Page

iv) Common Weakness Enumeration (CWE).
http://cwe.mitre.org/

v) United States National Institute of Standards and Technology (NIST), *Systems Security Engineering, SP 800-160*, Draft, May 2014.
http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

37 Provide and Use Audit *(1 September 2016)*

a) *The Company uses audit procedures to maintain internal compliance with enterprise direction and guidance.*

b) *The Company uses audit procedures to understand enterprise technical agreement with external compliance regimes, to which the Company must comply and report.*

c) *The Company uses audit reports to verify risk assessments and risk conditions.*

d) *The Company's audit personnel protect information assets and watch for cybersecurity discrepancies or threats during audit events.*

The Company uses testing and audit methods to verify that policies, procedures and practices follow Company direction and guidance. Both internal and external audit work efforts are valuable.

Technology system and security control audits are meant to check assumptions, validate the continued requirement for controls in place, and verify that security methods meet the Company's requirements. Audits can show where inertia ('always done it that way') can be replaced by new methods.

37.1 References

i) United States National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53 Rev 4*, Apr 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

ii) United States National Institute of Standards and Technology (NIST), *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, SP 800-53A Rev 4*, Dec 2014. http://csrc.nist.gov/publications/nistpubs/800-53A-rev4/sp800_53a_r4_errata_12_18_2014.docx

iii) United States National Institute of Standards and Technology (NIST), *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, SP 800-137*, Sep 2011. http://dx.doi.org/10.6028/NIST.SP.800-137

iv) United States National Institute of Standards and Technology (NIST), *Guide to Computer Security Log Management, SP 800-92*, Sep 2006. http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf