COLONIAL COMPLIANCE SYSTEMS, INC.
MARITIME REGULATORY CONSULTANTS

February 24, 2021

CSI Client Advisory 04-2021

SUBJECT: CYBER RISK MANAGEMENT

The U.S. Coast Guard recently released a Work Instruction on Cyber Risk Management and this has potential to impact your vessels calling US ports. The Work Instruction is attached, and this provides insight on how Coast Guard Port State Control Officers (PSCO) will proceed with the review of 'cyber hygiene' onboard your vessels.

The U.S. Coast Guard has incorporated both "*Guidelines for Port State Control Officers on the International Safety Management (ISM) Code*," **MSC-MEPC.4/Circ.4** as well as Maritime Safety Committee / Facilitation Committee Circular 3 "*Guidelines on Maritime Cyber Risk Management*," **MSC-FAL.1/Circ.3**. The latter reference gives high-level recommendations to stakeholders on assessing and mitigating cyber risks using five functional elements, which include:

1. **Identify** roles and responsibilities
2. **Protect** by having planning processes in place
3. **Detect** cybersecurity events in a timely manner
4. **Respond** quickly to provide resiliency and restore impacted systems
5. **Recover** by having backup systems to restore loss information

It is imperative that if you have vessels calling US ports to ensure cyber risk management is appropriately addressed in your SMS no later than your first annual verification of your Document of Compliance (DOC) after January 1, 2021. We anticipate the Coast Guard will commence checking 'cyber hygiene' during the course of their Port State Control exams.

Cyber risk management should already be incorporated into your vessel's SMS. If they identify that it is not, and the 2021 DOC verification audit has been completed, the Coast Guard inspectors are guided to issue a ***code 30 – ship detention*** with an external audit to follow within 3 months or prior to the ship returning to the US after sailing foreign. If deficiencies are found, PSCOs are directed to issue a ***code 17 – Rectify Prior to Departure*** with an internal audit requirement within 3 months or prior to returning to US port after sailing foreign. Lastly, if a '***serious'*** failure with cyber risk management is discovered that directly results in an impact to ship operations, PSCOs are guided to issue a ***code 30 – Ship Detained*** with the same auditing requirements as outlined above.

If you suspect or know you have had a cybersecurity event and/or incident, it needs to be reported immediately the U.S. Coast Guard National Response Center (NRC).

Should you have any questions regarding cyber security, please contact our office. This Client Advisory, along with previously issued CSI Advisories, can be retrieved from our website, www.compliancesystemsinc.com.

USCG Office of Commercial Vessel Compliance (CG-CVC)
Mission Management System (MMS) Work Instruction (WI)

Category	Commercial Vessel Compliance (Domestic and Foreign Vessels)				
Title	Vessel Cyber Risk Management Work Instruction				
Serial	CVC-WI-027(2)	Orig. Date	27OCT20	Rev. Date	18FEB2021
Disclaimer:	This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is not intended to nor does it impose legally binding requirements on any part. It represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the public, and the Coast Guard, as well as other federal and state regulators, in applying statutory and regulatory requirements. You can use an alternative approach for complying with these requirements if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative approach (you are not required to do so), you may contact the Coast Guard Office of Commercial Vessel Compliance (CG-CVC) at CG-CVC@uscg.mil who is responsible for implementing this guidance.				
References:	(a) Maritime Safety Committee Resolution 428(98), "Maritime Cyber Risk Management in Safety Management Systems" (b) U.S. Coast Guard Cyber Strategy, June 2015 (c) International Safety Management (ISM) Code (d) U.S. Flag Interpretations on the ISM Code, (CVC-WI-004(1)) (e) Title 33 Code of Federal Regulations (CFR) Part 96 (f) Chapter IX, Management of the Safe Operation of Ships, International Convention for the Safety of Life at Sea (SOLAS), 1974 (g) Title 33 Code of Federal Regulations (CFR) Subchapter H (h) National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, April 16, 2018 (i) Navigation and Vessel Inspection Circular (NVIC) 04-05: "Port State Control Guidelines for the Enforcement of Management for the Safe Operation of Ships (ISM Code)" (j) "Guidelines for Port State Control Officers on the International Safety Management (ISM) Code," MSC-MEPC.4/Circ.4 (k) USCG Oversight of Safety Management Systems on U.S Flag Vessels, (CVC-WI-003(1)) (l) Maritime Safety Committee / Facilitation Committee Circular 3 "Guidelines on Maritime Cyber Risk Management," MSC-FAL.1/Circ.3 (m) USCG Assistant Commandant for Prevention Policy (CG-5P) Policy Letter 08-16 " Reporting Suspicious Activity and Breaches of Security"				

A. Purpose. Reference (a) calls for Safety Management Systems required under the ISM Code to address cyber risks. This work instruction (WI) provides guidance regarding the U.S. Coast Guard (USCG) commercial vessel compliance program's approach to assessing the cyber risk on vessels to ensure vessels do not pose a risk to the Marine Transportation System (MTS) due to a cyber event.

B. Action. Marine Inspectors (MIs) and Port State Control Officers (PSCOs) should be familiar with reference (b) and use the guidance provided in this WI to evaluate how well a vessel's Safety Management System (SMS) complies with references (a) and (c-f). Additionally, this WI provides guidance to MIs when assessing cyber risk management onboard non-SMS U.S. vessels. Lastly, this WI discusses use of COTP orders and CG-835Vs to control vessels that have been affected by a cyber incident, and responding to a reported or probable cyber incident affecting the seaworthiness of a vessel.

U.S. flagged vessels subject to reference (c) are required to evaluate cyber risk and establish procedures to respond to a cyber-attack as per reference (d). Starting January 1, 2021, all vessels with a Safety Management System (SMS) pursuant to reference (a) should address cybersecurity risk

with respect to references (c) and (e). The January 2021 requirement also applies to vessels that voluntarily comply with reference (e).

C. Background. As maritime operations become more reliant on the systems integrated through automation, cyber risk is an area of increasing concern in the Marine Transportation System. The USCG recognizes that not all shipping companies and ships are alike, and therefore the SMS provides shipping companies the ability to tailor a structured system to address evolving cybersecurity vulnerabilities unique to a company/vessel's specific management and operations.

1. MSC-FAL.1/Circ 3. Reference (l) contains high-level recommendations to maritime stakeholders on assessing maritime cyber risk management. This IMO circular refers to several standards to help identify and mitigate cyber risks, including five functional elements consistent with the NIST Framework:

   a. Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, post risks to ship operations.

   b. Protect: Implement risk control processes and measures, and contingency planning to protect against cybersecurity events and ensure continuity of shipping operations.

   c. Detect: Develop and implement activities necessary to detect a cybersecurity event in a timely manner.

   d. Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

   e. Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cybersecurity event.

2. Other international organizations (ISO/IEC), including shipping associations (BIMCO), have provided maritime cybersecurity guidance and best practices for industry stakeholders. A MI/PSCO may encounter a vessel managing cyber risk using these standards in lieu of the NIST framework.

D. Definitions.

1. *Company Security Officer (CSO).* The person designated by the Company as responsible for the security of the vessel, including implementation and maintenance of the vessel security plan, and for liaison with their respective Vessel Security Officer and the USCG (reference g).

2. *Cybersecurity.* The prevention of damage to, unauthorized use, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. This includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, communications systems and control systems required for safe shipboard navigation and operations (annotated from reference m).

3. *Cybersecurity Event.* A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation (reference h).

4. *Cybersecurity Incident.* Actions taken through the use of a computer networks that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein (reference m).

5. *International Safety Management (ISM) Code*. The International Management Code for the Safe Operation of Ships and Pollution Prevention, Chapter IX of the Annex to the International Convention for the Safety of Life at Sea (SOLAS), 1974 (references c and e).

6. *Major non-conformity.* An identifiable deviation, which poses a serious threat to personnel or vessel safety or a serious risk to the environment and requires immediate corrective action. The lack of effective and systematic implementation of an ISM Code requirement is also considered a major non-conformity (reference c and e).
7. *Non-conformity.* An observed situation where objective evidence indicates the non-fulfillment of a specified requirement (reference c and e).
8. *Objective Evidence.* Quantitative or qualitative information, records or statements of fact pertaining to safety or to the existence and implementation of a SMS element based on observation, measurement or test and which can be verified (reference c and e).
9. *Safety Management System (SMS).* A structured and documented system enabling company and vessel personnel to effectively implement the responsible person's safety and environmental protection policies (reference c and e).
10. *Vessel Security Assessment (VSA).* An analysis that examines and evaluates the vessel and its operations taking into account possible threats, vulnerabilities, consequences and existing protective measures, procedures and operations (reference g).
11. *Vessel Security Plan (VSP).* A plan developed to ensure the application of security measures designed to protect the vessel and the facility that the vessel is servicing or interacting with, the vessel's cargoes and persons on board at the respective Maritime Security (MARSEC) levels (reference g).
12. *Vessel Security Officer (VSO).* The person onboard the vessel who is accountable to the Master and designated by the Company as responsible for the security of the vessel, including implementation and maintenance of the vessel security plan, and for liaison with their respective Company Security Officer and the Facility Security Officer (FSO) (reference g).

E. Discussion.

1. Per reference (d), as a Flag Administration, the USCG expects that U.S. flagged vessels and companies will incorporate cyber risk management into their SMS. Additionally, as a port state, pursuant to reference (a), companies with foreign flagged vessels that call on ports in the U.S. should ensure cyber risk management is appropriately addressed in their SMS no later than the first annual verification of the company's Document of Compliance (DOC) after January 1, 2021.
2. This WI also contains guidance regarding those vessels that are not required to implement and maintain a SMS, but are required to maintain a VSP as per reference (g). MIs should keep in mind that a VSP might include measures taken to mitigate cyber related vulnerabilities that the ship would be required to follow in order to meet 33 CFR part 104. Owners and operators of a vessel required to maintain a VSP have until December 31, 2021 to implement measures to mitigate cyber related vulnerabilities.
3. For the purposes of this WI, USCG vessel compliance activities are only directed towards cyber risk management on systems that are critical to the safe operation and navigation of the vessel. Stand-alone computers or other systems which do not affect the safe operation or navigation of the vessel are not to be inspected or examined.

F. Vessels subject to the ISM Code (U.S. & Foreign Vessels).

1. Basic Cyber Hygiene. The MI/PSCO shall identify when basic cyber hygiene procedures are not in place onboard. These include, but not limited to the following:

   a. Poor cyber hygiene

      1) Username / Password openly displayed

2) Computer system appears to require a generic login or no login for access

3) Computer system does not appear to automatically log out after extended period of user inactivity

4) Heavy reliance on flash drive/USB media use

b. Shipboard computers readily appear to have been compromised by ransomware/excessive pop-ups

c. Officers/crew complain about unusual network issues and reliability impacting shipboard systems

d. Unit/vessel screener received potential 'spoofed' email from master/crew onboard.

If these observations are not directly linked to statutory requirements or are not technical or operational-related deficiencies, the MI/PSCO does not have clear grounds to conduct a more detailed inspection. However these vulnerabilities should be discussed directly with the master. In addition, these discussions shall be annotated in the MISLE inspection narrative and documented with a deficiency entered into MISLE marked "Worklist Item/Do Not Show in PSIX" for data analysis.

2. Guidance for assessing cybersecurity onboard a vessel subject to the ISM Code. During the course of a normal inspection/examination, the MI/PSCO should evaluate whether or not a cybersecurity event was a factor in the failure of a system required for the safe navigation or operation of the vessel.

Example: While aboard a ship for a PSC exam the 2nd Officer explains that the ECDIS is not operational after a recent electronic chart update. The PSCO asks the 2nd Officer what is the procedure to update the ECDIS? The 2nd Officer explains that the ECDIS is updated via a flash drive loaded with updates from a shipboard computer (this scenario continues throughout the work instruction).

Up to this point the PSCO is still trying to determine why a piece of equipment required for the safe navigation of the vessel is not operating properly. SOLAS Regulation V/27 requires all nautical charts necessary for the intended voyage shall be adequate and up to date. Since the ECDIS is not operational, the applicable SOLAS Regulation is not met.

(Example continued) The PSCO continues by querying the 2nd Officer if the flash drive was scanned for viruses/malware prior to connecting to the ECDIS, and they state "no." At this point, poor cyber hygiene may have occurred and the PSCO has established clear grounds to conduct a more detail exam including the cyber risk management portion of the SMS.

3. More Detailed Inspection (Expanded Exam). If clear grounds are established, the MI/PSCO should conduct a more detailed inspection consistent with the applicable guidance for a foreign or U.S. vessel in accordance with reference (j) or (k), respectively. Based on objective evidence, the MI/PSCO may discover and can issue deficiencies based on the portion of the SMS that is not being effectively implemented with respect to cyber risk management. A more detailed inspection does NOT automatically mean that an ISM deficiency exists. MI/PSCO should NOT direct the ship to create any checklists or procedures with respect to cyber risk management. A MI aboard a U.S. vessel may review internal audits and corrective action reports while conducting a more detailed inspection.

(Example continued) The PSCO reviews the cyber security portion of the vessel's SMS. The SMS requires all thumb drives to be scanned for malware prior to connection to a ship's

computer/system. Since the 2nd Officer has already stated that the thumb drive was not scanned, there exists an ISM deficiency.

4. Deficiencies. If objective evidence is identified indicating that the vessel failed to implement its SMS with respect to cyber risk management, the MI/PSCO should direct the vessel to take the following actions:

   a. For U.S. Vessels:

      1) MIs should follow the guidance in reference (k) which sets forth guidance for assessing the effectiveness of a company's SMS on U.S. flag vessels

   b. For Foreign vessels:

      1) If cyber risk management has not been incorporated into the vessel's SMS by the company's first annual verification of the DOC after January 1, 2021, a deficiency should be issued with action code *30 – Ship Detained*, with the requirement of an external audit within 3 months or prior to returning to a U.S. port after sailing foreign.

      2) When objective evidence indicates that the vessel failed to implement its SMS with respect to cyber risk management, then the PSCO should issue a deficiency for both the operational deficiency and an ISM deficiency with an action code 17 – *Rectify Prior to Departure* and require the vessel to conduct an internal audit, focused on the vessel's cyber risk management, within 3 months or, prior to returning to a U.S. port after sailing foreign.

      3) When objective evidence indicates there is a serious failure to implement the SMS with respect to cyber risk management that directly resulted in a cybersecurity incident impacting ship operations (e.g. diminished vessel safety/security, or posed increased risk to the environment), after gaining concurrence from the OCMI, the PSCO should issue a deficiency for both the operational deficiency and an ISM deficiency with action code 30 – *Ship Detained* with the requirement of an external audit within 3 months or prior to returning to a U.S. port after sailing foreign.

   c. With the exception of U.S. vessels described in a.1 above, deficiencies issued with respect to ISM and cybersecurity should be assigned deficiency code 15113 (Other ISM) on the respective deficiency form (PSC Form B) and entered into MISLE marked "Worklist Item/Do Not Show in PSIX" and include the word 'CYBERSECURITY-ISM' at the beginning to aid with data analysis.

G. Non-SMS U.S. Vessels subject to MTSA.

1. VSA. A vessel owner or operator must consider cybersecurity vulnerabilities when conducting the vessel's VSA in accordance with 33 CFR 104.305. Cybersecurity vulnerabilities should be addressed per 33 CFR 104.305(d)(2)(v) and 33 CFR 104.305(d)(2)(vi). Owners and operators have until December 31, 2021 to address cybersecurity vulnerabilities within their VSA.

2. Questions for MIs to ask during Maritime Transportation Security Act (MTSA) Verifications.

   a. *Does your VSP address measures taken to address cybersecurity vulnerabilities?*

      - If yes: *Are these measures in place?*

         1) If yes: No further action/questions.

         2) If no, then ask: *Have you communicated that issue to your CSO?*

            i. If yes: No further action/questions required.

            ii. If no: Issue deficiency as per paragraph G.3 below.

- If no, then ask: *Has the vessel experienced any cybersecurity events[1] within the past 12 months?*

  1) If yes, then ask: *Have you reported these cybersecurity incidents to your CSO?*

     i. If yes: Reasonably verify reporting to CSO, then no further action.

     ii. If no: Issue deficiency as per paragraph G.3 below.

  2) If no: No further action/question required.

3. Issuing Deficiencies for cyber-related issues. As per the guidance in the paragraph above, MIs should issue a deficiency (Code 50; 30 days to rectify) on an CG-835V directing the VSO to submit cyber-related issues to the CSO as per 33 CFR 104.215(e). Deficiencies issued as described above with respect to MTSA and cybersecurity should be assigned deficiency code 16107 (Other Maritime Security) on the CG-835V and MISLE. The MI shall ensure that the "Security Violation" is checked for the deficiency in MISLE to prevent inadvertent release of Sensitive Security Information (SSI). The deficiency description in MISLE must include 'CYBERSECURITY-MTSA' at the beginning to aid with the data analysis.

H. Considerations for all reportable marine casualties. When attending a vessel for a damage survey, in-service inspection or port state control exam following a report of a marine casualty (as defined by 46 CFR 4.05-1) the MI/PSCO or Investigating Officer (IO) should always consider the possibility of the incident being related to a cybersecurity event in cases where system/equipment failure have no obvious causes. MIs/PSCO/IO should utilize the procedures outlined above to assist with this determination. The MI/PSCO/IO should determine if there was a failure of a system required for the safe navigation or operation of the ship, and then determine if it was a cybersecurity event. After making this determination, the MI/PSCO/IO ensure that the owner or operator promptly report the incident to the National Response Center (NRC) or the Department of Homeland Security National Communications and Cybersecurity Information Center (NCCIC) to initiate a coordinated federal response.

I. Reporting of cybersecurity events. See reference (m) when determining if a cybersecurity event and/or incident needs to be reported by the vessel owner/operator to the NRC or NCCIC.

J. Responding to a cybersecurity event / cybersecurity incident / marine casualty. The OCMI may request CGCYBER Cyber Protection Team (CPT) support through the District/Sector Command Center when the cybersecurity incident has impacted the MTS (i.e. vessel unable to move from loading terminal, casualty that limits or prevents movement of other vessel traffic on the waterway). The CPT can be contacted via the CG Cyber Command watch at (202) 372-2904 or at CyberWatch@uscg.mil. A MI/PSCO should be prepared to attend a vessel when a cybersecurity event onboard has been deemed a cybersecurity incident (see definition above). An onboard attendance to the vessel may be necessary to evaluate whether vital systems for safety, security, and environmental protection have been affected by a cybersecurity incident or remain functioning as required. If these systems were impacted, then the MI/PSCO should take actions to ensure these vital systems are fully restored.

K. Captain of the Port (COTP) Order. The COTP order is most appropriate and effective tool for control of a U.S. or Foreign Flagged vessel experiencing a cybersecurity incident that impacts

[1] Examples of cybersecurity events include: Intrusions into telecommunications equipment, computer, and networked systems linked to security plan functions (e.g. access control, cargo control, monitoring), unauthorized root or administrator access to security and industrial control systems, successful phishing attempts or malicious insider activity that could allow outside entities access to internal IT systems that are linked to the MTS. Also, instances of viruses, Trojan Horses, worms, zombies or other malicious software that have a widespread impact or adversely affect one or more on-site mission critical servers that are linked to security plan functions.

systems necessary for the safe operation of the vessel. The COTP should issue the order in the same manner that a COTP order would be issued for inoperable essential shipboard equipment with an unknown cause (e.g. loss of propulsion or steering reported to the USCG prior to troubleshooting issue). The COTP order imposes the minimal vessel control actions necessary to limit the vessel's effect on the MTS or facility until the issue has been identified and corrective measures put in place. For example, if the vessel's propulsion system was potentially involved in a cybersecurity incident, the COTP order could direct the vessel to proceed to the nearest anchorage, utilize tug escort, or accept a master attestation indicating vital systems are operational for mooring/anchoring/cargo operations. COTPs should also consider the extent of the cyber event onboard when imposing vessel control actions. A cyber event that affects shipboard control systems is much more serious than a cybersecurity event onboard affecting a non-integrated shipboard computer/device (e.g. malware, virus, ransomware). For example, a ransomware affecting shipboard computers used for communicating with the shoreside company, arranging logistics and cargo operations may not require a COTP order for tugs or to direct the vessel to anchor. However, it may be appropriate to prohibit shoreside connections until the extent of the cyber event has been determined.

L. COTP Order vs. CG-835V. For the purposes of safeguarding the MTS, the COTP order is the most effective and primary tool for controlling a vessel experiencing a cybersecurity incident. A CG-835V may be issued to a U.S. vessel to require repairs or corrective action to a specific regulation.

M. Training. MIs/PSCOs shall view and understand the basic maritime cybersecurity principles in the Maritime Cybersecurity Webinar posted on the CG-FAC website. Additionally, MIs/PSCOs should have a basic understanding of reference (h), particularly how the framework would apply in the maritime setting.

N. Appeals. The appeal procedure for decisions made by the Officer in Charge of Marine Inspections (OCMI) is outlined in 46 CFR Subpart 1.03. The appeal procedure for decisions made by COTP, under 33 CFR Subchapter H, should follow the appeal procedures outlined in 33 CFR 101.420.

O. Questions. All questions and comments regarding this policy can be sent to the Office of Commercial Vessel Compliance at CG-CVC@uscg.mil (U.S. Flag Vessels) or PortStateControl@uscg.mil (Foreign Flag Vessels).

M. EDWARDS
Captain, U.S. Coast Guard
Chief, Office of Commercial Vessel Compliance
By direction

INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3
5 July 2017

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

***

ANNEX

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 INTRODUCTION

1.1 These Guidelines provide high-level recommendations for maritime cyber risk management. For the purpose of these Guidelines, *maritime cyber risk* refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

1.2 Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping.

1.3 For details and guidance related to the development and implementation of specific risk management processes, users of these Guidelines should refer to specific Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

1.4 Risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

1.5 Predicated on the goal of supporting safe and secure shipping, which is operationally resilient to cyber risks, these Guidelines provide recommendations that can be incorporated into existing risk management processes. In this regard, the Guidelines are complementary to the safety and security management practices established by this Organization.

2 GENERAL

2.1 Background

2.1.1 Cybertechnologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. In some cases, these systems are to comply with international standards and Flag Administration requirements. However, the vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which should be addressed. Vulnerable systems could include, but are not limited to:

.1 Bridge systems;
.2 Cargo handling and management systems;
.3 Propulsion and machinery management and power control systems;
.4 Access control systems;
.5 Passenger servicing and management systems;
.6 Passenger facing public networks;
.7 Administrative and crew welfare systems; and
.8 Communication systems.

2.1.2 The distinction between information technology and operational technology systems should be considered. Information technology systems may be thought of as focusing on the use of data as information. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes. Furthermore, the protection of information and data exchange within these systems should also be considered.

2.1.3 While these technologies and systems provide significant efficiency gains for the maritime industry, they also present risks to critical systems and processes linked to the operation of systems integral to shipping. These risks may result from vulnerabilities arising from inadequate operation, integration, maintenance and design of cyber-related systems, and from intentional and unintentional cyberthreats.

2.1.4 Threats are presented by malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions). In general, these actions expose vulnerabilities (e.g. outdated software or ineffective firewalls) or exploit a vulnerability in operational or information technology. Effective cyber risk management should consider both kinds of threat.

2.1.5 Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyberdiscipline. In general, where vulnerabilities in operational and/or information technology are exposed or exploited, either directly (e.g. weak passwords leading to unauthorized access) or indirectly (e.g. the absence of network segregation), there can be implications for security and the confidentiality, integrity and availability of information. Additionally, when operational and/or information technology vulnerabilities are exposed or exploited, there can be implications for safety, particularly where critical systems (e.g. bridge navigation or main propulsion systems) are compromised.

2.1.6 Effective cyber risk management should also consider safety and security impacts resulting from the exposure or exploitation of vulnerabilities in information technology systems. This could result from inappropriate connection to operational technology systems or from procedural lapses by operational personnel or third parties, which may compromise these systems (e.g. inappropriate use of removable media such as a memory stick).

2.1.7 Further information regarding vulnerabilities and threats can be found in the additional guidance and standards referenced in section 4.

2.1.8 These rapidly changing technologies and threats make it difficult to address these risks only through technical standards. As such, these Guidelines recommend a risk management approach to cyber risks that is resilient and evolves as a natural extension of existing safety and security management practices.

2.1.9 In considering potential sources of threats and vulnerabilities and associated risk mitigation strategies, a number of potential control options for cyber risk management should also be taken into consideration, including amongst others, management, operational or procedural, and technical controls.

2.2 Application

2.2.1 These Guidelines are primarily intended for all organizations in the shipping industry, and are designed to encourage safety and security management practices in the cyberdomain.

2.2.2 Recognizing that no two organizations in the shipping industry are the same, these Guidelines are expressed in broad terms in order to have a widespread application. Ships with limited cyber-related systems may find a simple application of these Guidelines to be sufficient; however, ships with complex cyber-related systems may require a greater level of care and should seek additional resources through reputable industry and Government partners.

2.2.3 These Guidelines are recommendatory.

3 ELEMENTS OF CYBER RISK MANAGEMENT

3.1 For the purpose of these Guidelines, *cyber risk management* means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.

3.2 The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks.

3.3 Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

3.4 One accepted approach to achieve the above is to comprehensively assess and compare an organization's current, and desired, cyber risk management postures. Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritized cyber risk management plan. This risk-based approach will enable an organization to best apply its resources in the most effective manner.

3.5 These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework:

.1 Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

.2 Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

.3 Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.

.4 Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

.5 Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

3.6 These functional elements encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange, and constitute an ongoing process with effective feedback mechanisms.

3.7 Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.

4 BEST PRACTICES FOR IMPLEMENTATION OF CYBER RISK MANAGEMENT

4.1 The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyberthreats and vulnerabilities. For detailed guidance on cyber risk management, users of these Guidelines should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

4.2 Additional guidance and standards may include, but are not limited to:[1]

.1 The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

.2 ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

.3 United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure *Cyber*security (the NIST Framework).

4.3 Reference should be made to the most current version of any guidance or standards utilized.

---

[1] The additional guidance and standards are listed as a non-exhaustive reference to further detailed information for users of these Guidelines. The referenced guidance and standards have not been issued by the Organization and their use remains at the discretion of individual users of these Guidelines.