Chapter 32: Toward a Maritime Cyber Security Compliance Regime

Mark R. Heckman, John McCready, David Mayhew, and Winnie L. Callahan

University of San Diego

Abstract

This whitepaper is an attempt at understanding, bounding, and providing a framework for answering the following questions posed by the United States Coast Guard: *What actions should vessel owners and port entity operators perform to evaluate their cyber safety and security postures (perhaps within the context of MTSA)? How can these steps be validated and who, if anyone, should do so and how often? How can we measure the effectiveness of a compliance regime that requires these types of performance-based protection measures?* The paper discusses cyber security standards and compliance regimes in general, risks specific to the maritime transportation system, current efforts by the USCG and other entities, the feasibility of a USCG-led maritime compliance regime, and directions for future research.

Introduction

The 2013 Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, promotes a national policy to "strengthen and maintain secure, functioning, and resilient critical infrastructure" (White House 2013b). Critical infrastructure is defined in Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (White House 2013a). One of the 16 critical infrastructure sectors identified in PPD-21 is Transportation Systems. The sector specific agencies (SSA) tasked with overseeing the Transportation Systems sector effort, the Department of Homeland Security (DHS) and the Department of Transportation (DOT), identified 7 key subsectors, one of which is the Maritime Transportation System (MTS) (U.S. Department of Homeland Security 2016). Under the DHS and DOT's *Transportation Systems Sector-Specific Plan* (TS SSP), DHS delegated its co-SSA responsibilities to the Transportation Security Administration (TSA) and the United States Coast Guard (USCG) (U.S. Department of Homeland Security 2015c).

Cyber systems in the MTS are intricately linked to physical systems and provide attackers an increased attack surface beyond the primarily physical vectors addressed by existing regulations such as the International Ship and Port Facility (ISPS) Code and Federal regulations that implement the Maritime Transportation Security Act (MTSA) (Office of the Federal

Register 2003; International Maritime Organization 2016). One of the goals of the TS SSP is to further the implementation of EO 13636, in recognition of the increasing reliance by transportation services on networked and often remotely-accessible cyber-based systems for "positioning, navigation, tracking, shipment routing, industrial system controls, access controls, signaling, communications, and data and business management." Frequent reports of the ease with which attackers have been able to penetrate and exploit similar types of systems in other government and commercial sectors increase the urgency of addressing these new threats.

A major objective in the 2015 *United States Coast Guard Cyber Strategy* is to reduce cyber vulnerability for vessels and facilities. (U.S. Coast Guard 2015). Achieving this objective will require the USCG to "Develop guidance for commercial vessel and waterfront facility operators on how to identify and evaluate their cyber security-related vulnerabilities [and] incorporate this risk information into existing vessel and facility security assessments, or other appropriate management regimes, conducted by private industry and port authorities." The USCG asked the University of San Diego (USD) to explore the form that an organized program that provided such guidance and assessments might take. Specifically, the questions posed by the USCG to USD were:

> *What actions should vessel owners and port entity operators perform to evaluate their cyber safety and security postures (perhaps within the context of MTSA)? How can these steps be validated and who, if anyone, should do so and how often? How can we measure the effectiveness of a compliance regime that requires these types of performance-based protection measures?*

An evaluation of the cyber safety and security posture of a vessel or port facility, however, is likely to always return "not secure" unless the vessel or port facility operator takes specific actions to improve the posture. A cyber security compliance regime evaluates the security posture of an entity by comparing the security practices of the entity against a security standard. So a more pertinent formulation of the questions might be this:

> *What practices should vessel owners and port owner operators adopt in order to raise their security postures to a minimally acceptable level? How can their efforts be validated and by whom, and how frequently should evaluations be performed? How can the effectiveness of the compliance regime that validates the security efforts be measured?*

This whitepaper is an attempt to understand, bound, and provide a framework for addressing these questions. It incorporates feedback from a November 16, 2016 working meeting of the Maritime Cyber Security USCG/University Research Initiative on an earlier draft. The following sections discuss cyber security standards and compliance regimes in general, risks specific to the MTS, current efforts by the USCG and other entities, the feasibility of a USCG-led maritime compliance regime, and directions for future research.

Compliance Regimes

A compliance regime is a set of processes that ensure an organization and its systems are compliant with a set of obligations, usually regulatory obligations. The regime must include a

standard or set of standards and processes for evaluating compliance against the standards, for resolving deficiencies found during an evaluation, and for maintaining compliance between evaluations. Additional processes are usually required for record-keeping and reporting results to the compliance enforcement agency. The USCG, for example, under Federal regulations to enact provisions of the MTSA (Office of the Federal Register 2003), administers a compliance regime for U.S. enforcement of the International Convention for the Safety of Life at Sea (SOLAS) and the International Ship and Port Facility (ISPS) Code (International Maritime Organization 2016). Many aspects of this regime may also serve as a model for a maritime cyber security compliance regime.

Compliance regimes are widely used for evaluating the security of cyber systems in many different sectors. Examples include the Payment Card Industry Data Security Standard (PCI-DSS) (Payment Card Industry 2016), required of all businesses that handle credit-card payments; the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards used to assure the reliability of the bulk power system in North America (North American Electric Reliability Corporation 2016b), which have been adopted by the Federal Energy Regulatory Commission (FERC) of the U.S. Department of Energy (DOE) as a mandatory standard; and the Department of Health and Human Services (HHS) Health Information Portability and Accountability Act (HIPAA) security and privacy rules, which apply to all health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form (HIPAA Security Rule 2016).

Compliance Regime Attributes

In addition to the standards and processes used to assess compliance, a compliance regime is characterized by several attributes:

- Is compliance mandatory or voluntary?
- Responsibility for enforcement
- Responsibility for auditing and reporting
- Penalties for non-compliance
- Period between audits

Mandatory versus Voluntary Compliance

A cyber security compliance regime may be mandatory, required by government statute or regulation, or it may be voluntary, where entities in a particular sector voluntarily impose a compliance regime on themselves because the entities recognize and seek to mitigate risk (and, perhaps, to forestall a government-mandated regime). HIPAA is an example of a mandatory compliance regime required by laws and regulations. PCI-DSS is a voluntary commercial sector initiative mandated by credit card companies, not by a government entity. NERC CIP was originally a voluntary regime that has become a mandatory regime under FERC.

Because the MTS is critical infrastructure, it is logical that a maritime cyber security compliance regime will be mandatory, just as SOLAS and the ISPS Code are.

Responsibility for Enforcement

A compliance regime that has any teeth at all requires enforcement. An enforcement entity is responsible for carrying out control and compliance review measures and levying sanctions. The enforcement entity could be private, as in the PCI-DSS, or a government entity, as with HIPAA, or a private entity with the backing of a government entity, as with NERC and FERC.

The NERC/FERC paradigm may be a useful model for the USCG and the MTS. A private critical sector umbrella organization, NERC, developed a cyber security compliance standard and administers that standard under regulatory review and oversight of FERC. NERC has been certified by FERC for purposes of establishing standards, enforcement, and imposing sanctions for violations, and is required to submit an assessment of its performance to FERC every 5 years.

It is not clear, however, if there is any existing non- or quasi-governmental organization that currently has the authority, widespread acceptance, and technical knowledge to serve the same role in the MTS as NERC does in the electrical power sector. Perhaps the International Maritime Organization (IMO), which provides support and guidance for the SOLAS and the ISPS Code, comes closest. But the IMO is a treaty organization that does not enforce compliance. Enforcement in the U.S. is the responsibility of the USCG.

Under the MTSA, a USCG Captain of the Port (COTP) (also the District Commander, Area Commander, and the Commandant) has the authority to enforce provisions of SOLAS and the ISPS Code. Vessel and facility owners or operators must submit proof of compliance to the COTP, request a waiver, or face sanctions. Owners and operators may carry out their own security assessments and develop their own security plans, or they may hire and supervise third parties with "appropriate skills". The role of the USCG is to check the quality of the assessments and plans and to ensure that the facilities and vessels are adhering to the plans (Office of the Federal Register 2003).

Conceivably, the USCG could enforce cyber security compliance using a similar model. Owners or operators, or an independent third-party hired by them, would be responsible for conducting compliance evaluations and reporting results to the USCG.

Responsibility for Auditing and Reporting

Auditing and reporting of audit results may be performed by the audited entity or by an independent entity. Self-auditing and reporting suffers from the obvious weakness that organizations cannot always be trusted to accurately evaluate and report their security postures, especially if there are sanctions for non-compliance. (Self-reporting can be useful, however, to gain experience when a new regime is starting up.) Independent third parties, presumed to be unbiased and trained, generally give more reliable results.

Some compliance regimes, such as HIPAA, use self-auditing and reporting. Organizations subject to the HIPAA security rule must carry out periodic technical and non-technical evaluations to make sure that their security policies and procedures meet the security requirements. HHS does not care if the evaluation is made by the organization itself or by a third-party and there are no standards for certifying auditors. The PCI-DSS, on the other hand, requires formal compliance assessments by trained "Qualified Security Assessors" (QSAs) in certain cases, such as for merchants (or their service providers) who handle large numbers of transactions or that have been breached in the past. The PCI Security Standards Council provides training and certifies QSAs, but each organization can choose its own QSA to carry out an audit.

Each of the eight NERC regional entities keeps a list of contractor auditors who are deemed to have suitable training and experience and chooses which auditors are assigned to carry out an audit. NERC's approach of choosing the auditors ensures auditor independence and prevents organizations from "auditor shopping" in an attempt to more easily pass audits.

Because cyber security compliance is much more technical than the primarily physical compliance standards in the ISPS Code, adequate training and certification of evaluators will be critical for ensuring quality and consistency of evaluations. Creating a training and certification standard for evaluators will be an essential part of the creation of a maritime cyber security compliance regime. It is likely that, as with other cyber security compliance regimes, a commercial infrastructure of training courses and certifications will spring up as the regime matures, but certified evaluators should nevertheless be accredited by the enforcement agency (presumably the USCG).

Whether self-reported or reported by a third-party, results of an evaluation should be presented in a standard report format. And the compliance regime must provide some way for monitoring an organization's progress in addressing whatever deficiencies were found in an audit.

Penalties for Non-Compliance

Failure to comply with a mandatory regime may result in significant penalties. A business that is found not in compliance with the PCI-DSS, for example, may be forbidden from handling credit card transactions, which could severely hamper their operations. Sanctions for violations of NERC CIP include large monetary penalties and, in extreme cases, limitations on operations **Error! Reference source not found.** (North American Electric Reliability Corporation 2016b). And unauthorized disclosure of protected health information can lead to major fines by HHS **Error! Reference source not found.**(HIPAA Security Rule 2016).

Possible penalties under the MTSA for violations of SOLAS and the ISPS Code are as follows (Office of the Federal Register 2003):

1. Inspection of the vessel;
2. Delay of the vessel;
3. Detention of the vessel;
4. Restriction of vessel operations;
5. Denial of port entry;
6. Expulsion from port;
7. Lesser administrative and corrective measures; or
8. For U.S. vessels, suspension or revocation of security plan approval, thereby making that vessel ineligible to operate in, on, or under waters subject to the jurisdiction of the U.S. in accordance with 46 U.S.C. 70103(c)(5).

As cyber security is part of the overall security posture, these penalties may also be appropriate for violations of a maritime cyber security compliance regime.

Period between Audits

Allowing too much time between security evaluations may permit entities to grow lax with respect to compliance requirements, but audits are usually expensive and time-consuming efforts. PCI requires annual audits or security assessments, plus quarterly vulnerability scans (Payment Card Industry 2016). NERC Regional Entities typically conduct on-site audits every three years, but the results of "Inherent Risk Assessments" (IRAs) are used to scope the level of effort, so that some entities may only need to provide self-certifications or submit to spot-checks (North American Electric Reliability Corporation 2016a). Under certain conditions, however, based on the risk calculation, audits may be carried out more frequently (and FERC has begun to conduct its own random audits that are independent of NERC audits), so the period between audits can vary. The frequency of evaluations under a maritime cyber security compliance regime may be similarly variable, but that will depend on the nature of the regime and the standards used, and is still an open research question.

Cyber security Standards

The security of a system can only be evaluated for compliance against a standard or set of standards. Standards define the minimum set of security practices that an entity must adopt in order to be considered compliant. The level of compliance is a rough indicator of the entity's overall security posture. An essential first step in the creation of a maritime cyber security compliance regime, therefore, is creation of a set of standards against which compliance can be measured.

But standards only make sense in terms of helping entities to meet their organizational objectives (e.g., satisfy all relevant laws and regulations, be profitable, etc.) and enforcing a well-defined security policy against specific threats. Without a firm basis in policy and threats, a standard will likely have gaps that an adversary can exploit, or might contain unnecessary requirements that waste resources.

Security Policies

A security policy is the definition of security for a system. A system that correctly enforces the policy can be said to be "secure with respect to the policy". A security policy identifies the information that is to be protected, who is authorized to access the information, and the type of access that is authorized. Cyber security policies typically are concerned with the confidentiality of information (controlling who is allowed to read information), the integrity of information (maintaining the trustworthiness of information), and the availability of information (ensuring that information can be accessed and used when needed). The HIPAA security rule, for example, is primarily concerned with maintaining the confidentiality of protected health information. NERC CIP standards address confidentiality of sensitive data belonging to electricity sector infrastructure owners and operators, but focus primarily on the integrity of power grid components in order to maintain the reliability (availability) of the power grid.

Entities in the MTS have requirements for all three of these types of security policies. Development of a sound security policy is essential for creating a security program, and the security posture of a vessel or port facility can only be evaluated with respect to the specific policy that the vessel or facility is trying to enforce. So an essential first step in creating a maritime cyber security compliance regime will be to identify the types of information that must

be protected, who is authorized to access that information, and what types of access are authorized.

Threats, Vulnerabilities, and Risks

Threats are events or actions that can lead to a violation of a security policy. For example, a threat could be that an attacker will try to install malware on a system and thereby gain access to sensitive information, violating a confidentiality policy, or be able to tamper with the system and its data, violating an integrity policy. A vulnerability is a weakness in a system that could allow a threat to actualize. An unpatched operating system, for example, contains vulnerabilities that could be exploited to install malware.

An attack can be successful only when a threat meets a vulnerability. If there is no threat then a vulnerability does not matter and there can be no attack. If there is no vulnerability for a threat to exploit, there also can be no successful attack. Standards are written based on a threat model. The security controls in a standard are intended to eliminate or mitigate vulnerabilities so that threats cannot exploit them. That is why, for example, timely installation of operating system patches is always a part of cyber security standards. The patches eliminate vulnerabilities that could be exploited by threats.

A risk is an estimate of the potential impact of a successful attack. Risk estimates can be used to prioritize attention to protecting resources. If the cost of installing a particular security control exceeds the risk, it is not cost effective to install the control. The NIST Risk Management Framework (RMF) is a standard for protecting Federal information systems. Under the RMF, entities must determine the relative criticality of computing resources—low, medium, or high—with respect to confidentiality, integrity, and availability. The criticality level and the policy determine the number, type, and relative strength of security controls that must be used to protect each resource (National Institute of Standards and Technology 2010).

Good cyber security standards are based on policies, but also must consider threats, potential vulnerabilities, and risks to ensure that the security controls mandated by the standard are necessary and sufficient, and cost effective.

Descriptive and Prescriptive Standards

A standard may be descriptive or prescriptive. A descriptive standard specifies activities, but does not provide interpretation and specific implementation requirements. Examples are the "security rule" of HIPAA and the NERC standards. The HIPAA standards are intentionally high level and generic, so that different approaches can be used as technology evolves (HIPAA Security Rule 2016). The NERC CIP standards are also high-level and open to different interpretations, but NERC has found it necessary to provide detailed implementation guidance documents (North American Electric Reliability Corporation 2016c). At the other extreme, prescriptive standards are highly specific implementation rules. Examples of prescriptive standards are Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), which are exhaustive lists of system configuration settings for Department of Defense (DOD) information assurance (IA) and IA-enabled devices (Information Assurance Support Environment 2016). STIGs are part of the complete set of DOD compliance standards, which include both high-level, generic standards and the highly-specific STIGs.

As with the DOD, systems in the MTS will likely require both high-level, generic standards written so that they can still be effective as technology changes, but also highly detailed configuration standards for specific components.

Pros and Cons of Compliance Regimes

Compliance regimes, as with any human-designed system, have both advantages and disadvantages. Proper attention to processes and sanctions, however, can go a long way toward mitigating the disadvantages.

Advantages of Compliance Regimes

A compliance regime has many advantages as a defined program for focusing effort on a particular problem, such as cyber security. Some of these advantages are listed here:

- **Creates a definitive baseline for protection**—Compliance must always be measured against a standard. Creation of a compliance regime first requires creation of a clear and definitive security standard that is based on security policy, threats, and risk.
- **Improves cyber operations**—A well-designed cyber security standard focuses an entity's attention on secure configuration and management of cyber assets, which helps to normalize and streamline operations. For example, implementing a compliance regime encourages an organization to detect and identify previously unknown (and unapproved) cyber assets, to clean up tangled firewall rules that have accreted over time, and to implement monitoring that can detect changes to database schema, permissions, and dependencies.
- **Sets reasonable expectations**—Without a recognized and accepted standard, entities have no guidance about what a reasonable level of effort is.
- **Secures upper management buy-in**—Security is a very difficult property to measure. Organizations will often underestimate their risk and allocate too few resources to security in the absence of a measurable need. A compliance regime makes it possible to measure "success" (compliance with the standard) and to account for the cost of failure (the sanctions).
- **Drives budget into security departments**—Management will ensure that security departments have adequate resources to accomplish compliance. A compliance regime makes it possible for a security department to show, for example, how an expenditure of $100,000 can prevent a fine of $1,000,000, even in the absence of a detected breach.
- **Enhances interoperability and maintains security in networked entities**—Common, compatible security processes must be uniformly applied across distributed enterprises. Security is only as strong as the weakest link.
- **Improves communication and intelligence sharing**—Enterprises can share knowledge about breaches with partners who will be able to leverage their security controls to block attacks.
- **Creates efficiencies and economies of scale**—A security program based on a compliance regime requires a certain level of uniformity across the enterprise. Use of repeated, controlled processes create the opportunity for economies of scale.

- **Levels the playing field**—Entities that skimp on security may reap (temporary) benefits in terms of reduced expenditures, but a breach may have serious downstream effects and losses that extend well beyond that one entity. A compliance regime sets a minimum level of effort and forces everyone to shoulder part of the burden.
- **Increases customer confidence**—With major cyber security breaches being publicized almost daily, adherence to a strong compliance standard can increase customer confidence that the entity is taking appropriate steps to protect customer and entity assets.
- **Provides a defensible legal position in case of a breach**—Entities that are evaluated and found to be in compliance with an accepted cyber security standard may demonstrate that they are meeting a legal standard of due care with respect to cyber assets.
- **Provides a basis for insurers**—Cyber incident insurance is needed to help transfer risk. But insurers generally lack sufficient actuarial data to determine insurance rates. A compliance regime provides a standard that can be used by insurers as well as regulators.

Disadvantages of Compliance Regimes

While the advantages of compliance are marked enough to spark the creation of many such regimes, compliance regimes also have several weaknesses. It is imperative that the standards and processes that drive a regime mitigate the weaknesses in order to realize the advantages. Here are some of the weaknesses:

- **Compliance regimes can be expensive to implement and manage**—Organizations must maintain records, generate reports and, except when self-reporting is tolerated, support the work of an external auditor. The overhead of running a compliance regime may, in some cases, exceed the cost of the security controls themselves.
- **Regulations and standards only reflect current industry "best practices"**—"Best practices" are usually widespread and intuitive conventions, but historically have seldom had a scientific basis for assessing effectiveness. Once enshrined in a standard, they are very difficult to change.
- **Standards may lag well behind the latest attack vectors**—Yesterday's best practices may not reflect today's attacks, so standards require constant updating.
- **An organization can be totally compliant, yet completely unsecure**—As the saying goes, "compliance is to security what a dance-step diagram is to dancing." The result of a compliance audit is a checklist that reflects the conditions of an entity at a particular moment in time. Checklists measure the existence of controls, but it is very difficult to measure the quality of the controls. And the controls may not be vigorously implemented between audits.
- **Instead of being the floor, the standard becomes the ceiling**—Organizations may be tempted to do just the minimum necessary to pass a compliance audit. Security is no longer the goal; passing the audit becomes the goal.
- **Inconsistent auditing**—Training and experience of auditors can vary and compliance standards are often subjective, so auditors may disagree after evaluating the same system. If third-party auditors are paid by the organization under audit, the organization may "audit shop" until they find an easy auditor.

Measuring the Effectiveness of a Compliance Regime

The overall objective of a cyber security compliance regime is to improve the security posture of compliant organizations. But directly measuring "security" is not possible. If no successful breaches have been detected during some period of time, for example, is that because the security measures called for in the standards are effective against all attacks, because there just happened to have been no attacks of sufficient sophistication during that period of time that could get past the security measures, or because mechanisms for detecting successful attacks are too weak?

While "security" is impossible to measure, compliance with the security practices called for in the standards is intended to correlate with an improved security posture. And the reason for having a cyber security compliance regime, rather than simply having just standards, is to encourage or coerce organizations to adopt the security practices called for in the standards. A reasonable metric for the effectiveness of a compliance regime, therefore, is how well organizations comply with the standards over time. Effectiveness can be measured by counting the number of compliance deficiencies found during audits. Assuming a certain level of quality and consistency in evaluations, if the number of deficiencies found in each audit falls over time and reaches a steady, but low, level, the compliance regime can be counted a success because organizations are paying attention and making sure they are compliant. If the number of deficiencies continues to be high, however, the effectiveness of the regime may be called into question.

Another approach is to measure attributes of the security controls called for in the standards. Measurements may include, for example, counts of identified security vulnerabilities (which should drop over time) or the time it takes for an organization to respond to detected incidents. Metrics based on these measurements can be shown to be correlated with the effectiveness of the regime.

MTS-Specific Cyber Threats and Vulnerabilities

The primary cyber threats to the MTS are that attackers will attempt to (1) cripple ports; (2) track, divert, and disable vessels; and (3) disrupt cargo handling and tracking through attacks on information technology (IT) or computer-reliant systems. This risk is increasing along with "the growing reliance on cyber-based control, navigation, tracking, positioning, and communications systems" (U.S. Department of Homeland Security 2015c). The attack surface of maritime activities, formerly existing primarily in the physical realm, increasingly extends into the digital realm (and can be detected as failures across the digital to physical barrier). The USCG Office of Port & Facility Compliance suggests that cyber attacks could "kill or injure workers, damage equipment, expose the public to harmful pollutants, substantially slow cargo operations," and even "facilitate the smuggling of people, weapons of mass destruction, or other contraband" (U.S. Coast Guard 2016b).

Port Facility Cyber Threats and Vulnerabilities

Different vessels and port and terminal facilities, of different ages and with different levels of resources, may have widely varying dependence on cyber resources. It is, therefore,

difficult to generalize what threats and vulnerabilities broadly apply throughout the sector. Cyber Guard attack/defend exercise simulations make it apparent, however, that all ports face many of the same type of threats:

- **General IT threats**—Similar to threats faced by other government and commercial offices, such as attacks on office and server systems, networks, and web sites. Attackers may, for example, steal, tamper with, or destroy key databases.
- **Threats to operational technology (industrial) networks and systems**—Port facilities and terminals are also industrial sites that include remote equipment control networks—i.e., industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, and equipment connected to them such as cranes, fuel dispensing or recovery components, and even a local power grid.
- **Threats to physical security systems**—Physical security systems, such as closed-circuit camera (CCTV) systems, are increasingly cyber-based and networked.

Vessel Cyber Threats and Vulnerabilities

Ship-builders are already demonstrating completely automated and autonomous vessels; the cyber threat to such vessels is obvious, as are the risks if command and control were lost. In many computer-based products, however, developers focus on features, time-to-market, and cost—security is usually an afterthought and serious vulnerabilities are detected long after the system is put into use. Given the risks, no automated, autonomous vessel should be permitted to operate unless the controls on the vessel have been demonstrated to comply with a rigorous cyber security standard. In the absence of clear compliance requirements, however, developers have even less incentive to build security into the product.

Contemporary vessels already have a variety of devices and systems that are becoming increasingly cyber-dependent. As with most cyber-based devices and systems, these were undoubtedly developed with little or no awareness of cyber threats. Here are some examples of these devices and systems, and some of the threats to them:

- **Navigation**—automatic identification system (AIS), electronic chart display and information system (ECDIS), global positioning system (GPS), Radar—Information provided by the AIS, such as unique identification, position, course, and speed, may be blocked or spoofed; ECDIS navigation charts may be destroyed or tampered with, or inputs from position, heading, speed and other navigation sensors may be blocked or altered; GPS satellite signals maybe spoofed or blocked, or the system may be tampered with and provide incorrect location data.
- **Propulsion and Steering**—Digital controls are at risk of subversion. Malicious software could interfere with propulsion causing improper commands at critical times (e.g., vessels in turning basins) or could cause incorrect reporting of critical engine/propulsion indicators such as low oil pressure or high inter-cylinder temperatures, which may not immediately destroy an engine but could result in increased maintenance needs and causing reliability and cost issues.

- **Vessel balance of control**—Fire and damage control, Environmental controls, Waste controls—Intruders can disable systems or commandeer them, potentially, for example, dumping fuel, bilge, or ballast.
- **Communications**—Communications systems are ubiquitous within the entire vessel, interacting with routine message traffic, personal communications between crew members and their families, as well as providing continual reporting on position, system performance, navigation, etc. Communications are now largely automated and digital and can be blocked, eavesdropped on, or spoofed.

Cargo Handling Threats and Vulnerabilities

Disruptions to cargo management systems could lead to destruction, hiding, and theft of cargo, or allow the entrance of dangerous or illegal cargo. Refrigerated cargo monitoring ("Reefer Tracking") readings, for example, may be blocked or falsified, leading to destruction of the cargo. Fluid cargo management systems, intended to prevent overfilling and accidental product discharge of ballast or productive tanks by monitoring parameters as filling speed and temperature, may be crashed, or false readings may be presented on the console, resulting in damage to the crew, vessel, port, environment, or even loss of life. Management systems implemented using radio-frequency identification (RFID) tags are subject to attacks that block, clone, or spoof the tags, which would make it impossible to reliably identify and track shipments.

Existing, Non-secure Technology

Ideally, each of the computer-reliant devices and systems used in the MTS would be securable (and have their own STIG for secure configuration), but because they were developed without cyber security in mind, that may not be possible with the current generation of these devices. Additional development standards will need to be created that specify requirements for security that can be built into new systems. The long active service life-span of equipment and the need for backward compatibility, however, may delay full implementation of development standards for a long time, but is a necessary goal. As newer, and more securable, equipment is adopted in vessels and ports, older, less secure systems will co-exist with the newer systems, creating vulnerabilities. External devices may have to be used to provide some protection, but because the base protocol themselves in most cases do not have a security component, redundant systems may need to be used to provide some assurance that the devices or systems have not been subverted.

Multiple Spheres of Regulation

The 2013 attack on Target stores began with an attack on a vendor that provided HVAC and refrigeration systems to Target (Krebs 2014). This demonstrates that the security of a system may only be as good as the security of the weakest system to which it connects.

The MTS has many stakeholders and multiple entities may control different facilities in a port—even within the same cargo terminal. The June 2015 United States Coast Guard Cyber Strategy mentions that Coast Guard systems and networks are subject to compliance with DOD IA and Intelligence Community policies and regulations, but that most of the MTS critical cyber infrastructure is owned and operated by local governments and private companies that are not

subject to the same compliance requirements (U.S. Coast Guard 2015). These different entities may have vastly different perceptions of cyber risk, different levels of resources to implement security controls, and different levels of cyber experience and training. Vessels may be flagged in many different countries, which also have the same disparities. This could complicate the creation of a broadly applicable maritime cyber security regime.

Existing MTS Cyber Security Programs

Both the DHS and the USCG have current active efforts to address cyber security risks. USCG efforts to create a maritime cyber security compliance regime, not surprisingly given the request to create this whitepaper, are still immature. The USCG has an office of port and facility compliance whose mission is to "provide clear and timely regulations, policy and direction to Coast Guard Operational Commanders and other maritime stakeholders to achieve maritime safety, maritime security and environmental stewardship" (U.S. Coast Guard 2016a). The Domestic Ports Division (CG-FAC-1) has a web site dedicated to cyber security (U.S. Coast Guard 2016b), but this site is still underdeveloped and, absent a true standard, only makes very general suggestions to, e.g., "conduct a risk assessment" and "identify and adopt best practices". A January 2015 public meeting titled "Guidance on Maritime Cybersecurity Standards" was an attempt to grapple with some of the same questions posed in this whitepaper, including "How can vessel and facility operators reliably demonstrate to the Coast Guard that critical cyber systems meet appropriate technical or procedural standards" (U.S. Department of Homeland Security 2014)? The resulting February 2015 "Guidance on Maritime Cybersecurity Standards" document, which seems to be an attempt to answer the questions posed in the meeting, contained answers limited to procedures and tools to prevent malware infection through USB drives (U.S. Department of Homeland Security 2015a).

The DHS has created a "Transportation Systems Sector Cybersecurity Framework Implementation Guide" that purports to "provide an approach for Transportation Systems Sector owners and operators to apply the tenets of the National Institute of Standards and Technology [NIST] Cybersecurity Framework to help reduce cyber risks" but the guideline is an extremely high-level document that will require significant interpretation to turn it into something actionable by port facility and vessel operators (U.S. Department of Homeland Security 2015b). It provides no specific controls and little more direction than the NIST framework itself.

The NIST cyber security framework is considerably more developed and NIST frameworks have been used in other government agencies, but a framework is not a worksheet. It is non-trivial to interpret and implement a framework, requiring significant resources and trained staff to translate the abstract activities into concrete tasks (National Institute of Standards and Technology 2014). We found no record of a successful application of the NIST framework to any MTS entity, although that could simply reflect a lack of publicity for such efforts.

The American Bureau of Shipping (ABS) has recently (September 2016) published a series of documents on Maritime cyber security, such as *Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations* and a *Guide for Cybersecurity Implementation For The Marine And Offshore Industries*. (American Bureau of Shipping 2016a; 2016b). While these documents draw heavily from NIST guides, they also reference documents from other sources, such as the European Union Agency for Network and Information Security (ENISA) and standards organizations such as the International Standards Organization (ISO), International Electrotechnical Commission (IEC), IEEE, ANSI, and others. These documents are

an attempt to tailor NIST and other standards to maritime cyber security. ABS intends this framework to serve as a certification standard, for which ABS will be the evaluator and certification-provider (American Bureau of Shipping 2016b).

Lacking a standard and compliance regime, additional maritime cyber security controls are appearing to satisfy a need that is increasingly evident to stakeholders. An example is the Norman SCADA Protection (NSP) system being marketed by Kongsberg Maritime to protect Kongsberg Maritime systems (used for positioning and navigation, marine automation, cargo management, and other maritime functions) from malware (Kongsberg 2012). The Kongsberg NSP was cited in the February 2015 USCG "Guidance on Maritime Cybersecurity Standards" document (U.S. Department of Homeland Security 2015a).

Additional informal and ad-hoc guidelines are developing as concern for maritime cyber security grows without a definitive standard. The results of the most recent Cyber Guard exercise, for example, identified a few key take-aways (Parsons 2016):

- Network segmentation—can apply more stringent controls to critical resources
- Intrusion detection and correlation—to identify attack vectors and compromised systems
- Credential protection (e.g., passwords) —Use two-factor
- Federal partnership—Work with partnering agencies (expertise, intelligence) and have regular exercises

These findings, however, hardly constitute a standard.

A March 2016 presentation to a large international shipping container group could only advise that, until maritime cyber security standards are developed, the group should take the following actions (K & L Gates 2016):

- Know Your Systems
- Assess Their Vulnerabilities
- Design/Install Cyber security Protections
- Educate Your Workforce
- Reassess/Strengthen Defenses Regularly
- Establish/Practice Response/Remediation Team
- Stay Abreast of USCG/IMO Standards
- Choose Insurance That Fits Your Needs/Risks

Once again, it is clear that a demand exists among sector entities for a MTS standard, but there is little in the way of progress toward a widely accepted and actionable standard.

Feasibility of a MTS Cyber Security Compliance Regime

It seems logical that the USCG has the authority to mandate a maritime cyber security compliance regime. Furthermore, it is clear that there is already a recognized need for a maritime cyber security standard, not only by the USCG, but also by port, terminal, and vessel operators, and likely by insurers. In the absence of a standard, operators are grasping at different informal and ad-hoc guidelines, while at least one private organization has created its own maritime

standard. Given the demonstrated need, an official and well-designed standard and compliance regime could be an easy "sell" to operators and owners.

The span of authority of the USCG may not extend far enough to mandate full compliance with its standard to all terminal and vessel operators, however. Terminal operators have a certain amount of latitude with respect to how they run their operations, and foreign-flagged vessels have a great deal more. Compliance may start out mandatory for U.S. port facilities and vessels, but only recommended for others. Once a well-designed maritime cyber security standard becomes the U.S. standard, it could serve as a basis for international agreements under the IMO that would make compliance mandatory world-wide. A question for further research is what efforts other countries are making in this area and how those efforts could be combined with efforts in the U.S.

A comprehensive set of maritime compliance standards could be created as an interpretation of the NIST RMF tailored to protecting the MTS. Given the nature of the safety-critical devices and systems identified earlier, the standards would likely need to be a combination of high-level standards and STIGs. The feasibility to adopt or adapt previously created standards documents from other compliance regimes or from the ABS standard is still an open question, as is the full scope and shape of necessary standards.

The role of the USCG in enforcing the ISPS Code under the MTSA is oversight, approving standards, and reviewing and approving compliance. This is the same role the USCG would conceivably have in a new maritime cyber security compliance regime, and would probably not require a significant change in staffing or operations to manage the new regime. But managing a cyber security compliance regime requires different knowledge and skills than the primarily physical security regime of the ISPS Code, and will require new training for USCG personnel.

The issue of training applies just as much to port facility and vessel operators as it does to USCG personnel. A Vessel Security Officer training guide from a leading maritime training center that we reviewed, for example, contained no cyber security training (Vessel Security Officer Student Guide 2016). Cyber security practitioners are in great demand everywhere; it is highly unlikely that port facility staff and vessel crews would have these skills (large shipping companies, which have large IT departments, might be an exception). Other cyber security compliance regimes, however, have given rise to a vast infrastructure of training courses and certifications, as well as consultants, seeking to cash in on a lucrative market. It is certain that the same type of infrastructure will spring into existence around a maritime cyber security compliance regime as the regime matures.

Penalties for non-compliance with a maritime cyber security compliance regime could be very much like existing penalties for non-compliance under the MTSA. It is likely that any penalties, however, would be phased in gradually over time as standards are developed, tested, and adopted. This is the approach taken by, for example, the HHS under HIPAA, where penalties have gradually stiffened as organizations have had time to adapt to the new regulations.

As the preceding discussion shows, the form of a USCG-managed maritime cyber security compliance regime could be very similar to the way the USCG currently manages the current ISPS Code compliance regime, in terms of the USCG role, enforcement, and penalties. This suggests that a USCG-managed regime would be highly feasible. The specific standards that are to be enforced, however, are still an open research question.

Recommendations

A maritime cyber security compliance regime effort must begin with the creation of well-designed and actionable standards. The need for such standards is widely recognized because of increasing awareness about the risk of a cyber incident. Port facility and vessel operators are floundering without guidance.

But the MTS consists of a wide variety of cyber systems used for both business IT and industrial operations at ports and on vessels. There are existing cyber security compliance standards for business IT systems and even for SCADA systems that can be leveraged to create standards for maritime systems, but there are also unique aspects of the MTS that may not be addressed elsewhere. And there is no prior model for a vessel cyber security standard. Creating a comprehensive standard, even using a framework such as the NIST framework, will be a major undertaking.

Based on our findings, we recommend the following steps, in approximate order, for creating a comprehensive maritime cyber security compliance standard. Note that each of these steps is itself a research topic (or set of topics).

1. **Identify "organizational objectives" for cyber-based systems in the MTS**—This includes all relevant laws and regulations, as well as functional and performance goals.
2. **Create a complete inventory of cyber-based components (devices, networks, and systems) in the MTS**—No comprehensive threat model can be developed without such an inventory. The inventory should be categorized to help identify the types of applicable security policies and controls. Example categories could be, for example, "hardware", "software", "human", etc., but the ontology to be used is an open research question.
3. **Identify the security policies that must be enforced for digital information in port facilities and vessels**—This will require identifying the types of information that must be protected and the access policy for each information type.
4. **Create a detailed threat model for each component individually and as systems of components in vessels and port facilities**—Each item has its own threats and vulnerabilities, but each item is also part of a larger system. The larger system inherits the weaknesses of each of the components and the composition of components may induce weaknesses not present in the individual components.
5. **Create a risk model based on the threats and known or potential vulnerabilities**—The risk model must consider the impact on particular components and systems, vessels, or port facilities, but also to the MTS as a whole based on the downstream effect of a cyber attacks.
6. **Develop cyber security standards for base systems and protocols**—Standards for configuring and managing existing devices and protocols in order to mitigate threats should be created and the threats that cannot be mitigated should be documented. New equipment and systems should be required to have security built-in to address the threats. (Getting acceptance for standards that all new systems must adhere to, and for new, secure protocols, is likely to be a long-term project, however.) Existing standards from other sectors should be leveraged, when possible.
7. **Develop cyber security standards for port facilities, terminals, and vessels as whole systems**—These standards address the risks specific to the composition of cyber

components and extend over the entire entity. For example, insurance may be required to transfer residual risk when threats cannot be entirely mitigated.

8. **Foster the development of a cyber security curriculum that will become part of the required training of port and vessel personnel**—Tailor training to the needs of different staff positions.
9. **Require a cyber-component in all vessel and port security plans**—Security plans should identify responsible personnel and contain an incident handling plan that explains how a vessel's crew or a port's personnel would respond to a cyber-intrusion.

Conclusion

While the need for a maritime cyber security compliance standard is increasingly recognized, the decisions about how to create the standard and a regime built on the standard are still open research questions. Existing cyber security compliance standards and regimes in other critical sectors, such as NERC CIP in the power industry, should be studied and adapted when possible.

The creation of a cyber security compliance regime for a transportation sector is not a problem unique to the MTS. The Federal Aviation Administration (FAA), for example, is attempting to address cyber security issues in aircraft and airports. Aircraft are no longer "isolated and independent systems" but now are integrated into a large, distributed, networked system (U.S. Department of Transportation 2014). Consisting as the MTS does of a combination of IT, commercial, industrial, and communications systems, a MTS cyber security compliance regime is more likely to resemble that of other transportation sectors than it does of sectors, such as the financial sector, with more homogeneous systems. It is not clear if the FAA has yet developed a solution to this problem, but study of their progress to date could be illuminating.

In addition to the open research questions that surround the creation of compliance standards, there are also research questions about the compliance regime that would enforce the standards. The USCG has a well-developed process for managing and enforcing a physical security compliance regime. It may be possible to preserve this process for cyber security, although the nature of the risk is very different and would require different training for USCG staff who would assume the additional responsibility. Furthermore, cyber assets, vulnerabilities, and threats are constantly evolving. It may be necessary to review and update the cyber security compliance standards much more frequently than the physical security compliance standards. The frequency of assessments, too, may need in general to be higher than for physical security, and as with other compliance regimes, there may be specific events, such as detected breaches, that trigger assessments. These decisions, too, call for further study.

The only decision that does not need to be further studied is the decision to push ahead toward an actionable cyber security compliance standard and regime for the MTS. There is a growing gap that other entities have also recognized and are racing to fill, but without coordination the results will be confusing and wasteful. The USCG should lead and coordinate these efforts.

References

American Bureau of Shipping. 2016a. “Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations: ABS Cybersafety Volume 1.” (September). http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf

American Bureau of Shipping. 2016b. “Guide for Cybersecurity Implementation for the Marine and Offshore Industries: ABS Cybersafety Volume 2.” (September). http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/251_cybersafetyV2/CyberSafety_V2_Cybersecurity_Guide_e.pdf

HIPAA Security Rule. 2016. 45 CFR Part 160 and Subparts A and C of Part 164. (January 7). http://www.hhs.gov/hipaa/for-professionals/security/

Information Assurance Support Environment. 2016. “Security Technical Implementation Guides (STIGs).” (August 1). http://iase.disa.mil/stigs/Pages/index.aspx

International Maritime Organization. 2016. “Maritime Security.” http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Default.aspx (accessed January 7, 2017).

K & L Gates. 2016. “Maritime Cybersecurity, CMA Shipping 2016.” PowerPoint Presentation. (March 23).

Kongsberg. 2012. “Protecting Kongsberg Maritime IT Systems.” (June 8). https://www.km.kongsberg.com/ks/web/nokbg0238.nsf/AllWeb/FFD6EB66CE1EC4C2C1257A170028505C?OpenDocument (accessed January 7, 2017).

Krebs, Brian. 2014. “Target Hackers Broke in Via HVAC Company.” *Krebs on Security Blog.* (February 5). https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ (accessed January 7, 2017).

National Institute of Standards and Technology (NIST). 2010. “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.” Special Publication 800-37, Revision 1. (February). http://dx.doi.org/10.6028/NIST.SP.800-37r1

National Institute of Standards and Technology (NIST). 2014. “Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology.” (February 12). https://www.nist.gov/cyberframework (accessed January 7, 2017).

North American Electric Reliability Corporation. 2016a. “2016 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan.” Version 2.5. July. http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/2016%20CMEP%20IP_v_2%205_071116_POSTED.pdf

North American Electric Reliability Corporation. 2016b. “NERC Compliance & Enforcement.” http://www.nerc.com/pa/comp/Pages/default.aspx

North American Electric Reliability Corporation. 2016c. “NERC Compliance Guidance.” http://www.nerc.com/pa/comp/guidance/Pages/default.aspx

Office of the Federal Register. 2003. “Title 33 - Navigation and Navigable Waters.” (July 1). https://www.gpo.gov/fdsys/pkg/CFR-2003-title33-vol1/pdf/CFR-2003-title33-vol1.pdf and https://www.gpo.gov/fdsys/pkg/CFR-2003-title33-vol1/pdf/CFR-2003-title33-vol1-part101.pdf (accessed January 7, 2017).

Parsons, Jim. 2016. “Cyber Guard 16.” PowerPoint Presentation.

Payment Card Industry (PCI). 2016. “Data Security Standard: Requirements and Security Assessment Procedures.” Version 3.2. April. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

U.S. Coast Guard. 2015. *United States Coast Guard Cyber Strategy*. June. https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf (accessed January 7, 2017).

U.S. Coast Guard. 2016a. “CG-FAC Office of Port & Facility Compliance.” (October 6). https://www.uscg.mil/hq/cg5/cg544/default.asp

U.S. Coast Guard. 2016b. “Cybersecurity.” (October 6). https://www.uscg.mil/hq/cg5/cg544/cybersecurity.asp

U.S. Department of Homeland Security. 2014. “Supplemental Documents.” U.S. Coast Guard Cybersecurity Public Meeting. (December 17). https://www.regulations.gov/document?D=USCG-2014-1020-0002 (accessed January 7, 2017).

U.S. Department of Homeland Security. 2015a. “Guidance on Maritime Cybersecurity Standards.” U.S. Coast Guard Cybersecurity Public Meeting. Docket No. USCG-2014-1020. (February 18). https://www.regulations.gov/document?D=USCG-2014-1020-0016 (accessed January 8, 2017).

U.S. Department of Homeland Security. 2015b. “Transportation Systems Sector Cybersecurity Framework Implementation Guide.” (June 26). https://www.dhs.gov/publication/tss-cybersecurity-framework-implementation-guide (accessed January 8, 2017).

U.S. Department of Homeland Security. 2015c. “Transportation Systems Sector-Specific Plan 2015.” https://www.dhs.gov/publication/nipp-ssp-transportation-systems-2015 (accessed March 21, 2016).

U.S. Department of Homeland Security. 2016. “Transportation Systems Sector.” (July 8). https://www.dhs.gov/transportation-systems-sector (accessed January 7, 2017).

U.S. Department of Transportation. 2014. “A Summary of Cybersecurity Best Practices.” National Highway Traffic Safety Administration, DOT HS 812 075. (October). https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812075_CybersecurityBestPractices.pdf

Vessel Security Officer Student Guide. Training Resources, Ltd. Inc. Obtained October 2016.

White House. 2013a. “Executive Order -- Improving Critical Infrastructure Cybersecurity.” (February 2012). https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed January 7, 2017).

White House. 2013b. “Presidential Policy Directive -- Critical Infrastructure Security and Resilience.” PPD-21. (February 12). https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed January 7, 2017).