# Information Sharing for Maritime Cyber Risk Management

Dennis Egan, Darby Hering, Paul Kantor, Christie Nelson, Fred Roberts

April 18, 2016

**For further information: Dennis Egan, deegan@dimacs.rutgers.edu, or Fred Roberts, froberts@dimacs.rutgers.edu**

*Command, Control and Interoperability Center for Advanced Data Analysis*

A Department of Homeland Security University Center of Excellence

## Acknowledgements

The authors acknowledge vital discussions with CCICADA colleagues William Pottenger and Vanessa Kitzie in the course of this project. Special thanks go to our U.S. Coast Guard partners, in particular Mr. David Boyd, CAPT Michael Dickey, Dr. Joe DiRenzo III, LTJG Shanda Harper, LCDR Samuel Nassar, CAPT Andrew Tucci, CDR Brian McSorely, as well as the numerous U.S. Coast Guard and other government and private sector personnel whom we interviewed and are not specifically named. We would like to give a special acknowledgement to the two groups of reviewers who participated in the Working Meeting for Maritime Cyber Security, February 29 to March 2, 2016, and who contributed a number of new ideas and constructive criticisms that have been incorporated in the final version of this paper. CCICADA also gratefully acknowledges support from the Department of Homeland Security Office of University Programs, under award number 2009-ST-061-CCI002-07**.**

**Options for Maritime Cyber Risk Management Information Sharing**

Dennis Egan, Darby Hering, Paul Kantor, Christie Nelson, Fred Roberts

Table of Contents

## 1. Executive Summary

Effective and timely sharing of cyber risk management information among all stakeholders in the Maritime Transportation System (MTS) is vital to maintaining a safe, secure and resilient MTS. To develop information sharing protocols across this complex system, we must consider the layers of cyber risk management, including communication and technology, economic, and legal and regulatory aspects. Our research addresses the following questions: *What is the most appropriate role for the U.S. Coast Guard (USCG), and how does guidance for physical security relate to cyber risk management needs? What organizational systems could best support the needed sharing? What kinds of incentives could be used to encourage participation, particularly from private industry? What information needs to be shared, and when? What technologies could be used to enable and safeguard the information sharing?* In this white paper, we discuss the approach taken by the CCICADA-Rutgers team to address these topical questions. Our research process included interviews with experts, literature reviews, and taking a leadership role on the Port of New York and New Jersey Area Maritime Security Committee cyber subcommittee. We present our initial findings based on the interviews conducted and documents read, and we conclude with a set of recommendations related to each topical question.

## 2. The Background

At the March 2015 Maritime Cyber Security Symposium held at CCICADA/Rutgers University, one of the important themes was that the ability to share information in an effective and timely manner with all stakeholders in the MTS is essential in keeping the MTS safe, secure, and resilient. At the Symposium, VADM Charles Michel of the USCG laid out six research challenges. This paper deals with one of those challenges:

***Information Sharing*** - How would a framework for network analysis be developed to support optimal information sharing with partners to address maritime cyber issues?

In June 2015, a Maritime Cyber Security Research Summit was organized at California Maritime Academy to investigate these six research challenges. Working groups were formed to address each of the challenges and this led to a report (Clark and Roberts 2015).

After the report, three more focused research questions were posed by USCG-FAC (Office of Port and Facility Compliance). This report deals specifically with the following one of those questions:

***Information Sharing*** - Develop Information Sharing Protocols to meet the needs of industry and government.

To address this challenge, the CCICADA team set out to investigate methods to achieve rapid and useful information sharing in a way that both large and small players in the MTS can participate. In particular, how can we entice larger content providers to take the lead on information sharing within the MTS on cyber issues? We sought to explore ways to incentivize environments that are both transparent and candid in the sharing of information.

As part of the research, we also sought to investigate ways to categorize what information about the latest cyber threats and countermeasures should be shared and with whom. To answer this question we looked to understand the types of information that need to be shared rapidly as well as the types of information that do not impose an immediate threat. One example we set out to investigate is how and when to share reports on "near misses."

CCICADA also set out to understand what organizational structures for information sharing between government and industry in the MTS and between private sector MTS entities make the most sense to better understand:

- What information sharing leverage can be gained from existing organizations such as the Maritime Information Sharing and Analysis Center (M-ISAC) and Area Maritime Security Committees (AMSCs) or the National Cybersecurity and Communications Integration Center (NCCIC) or the International Maritime Organization (IMO) or NATO's Center for Combined Operations from the Sea (CJOS)?
- How is information sharing performed in other sectors such as those facilitating financial services, utilities, and oil and natural gas?
- Can we find good systems for use of real-time machine to machine interfaces such as the Security Information and Event Management (SIEM) software that can automatically collect, filter, correlate, vet, and distribute threat analysis and trends?

Finally, CCICADA sought to analyze the roles of the USCG in cyber risk management information sharing, roles such as developing standards for sharing systems, exchanging best practices, or enforcing sharing regulations. Can we learn a great deal from USCG reporting procedures for physical security risks, and translate those into good reporting procedures for cyber security risks?

This was an ambitious agenda for a project of a few months, and this paper reports on our preliminary findings and recommendations. There is a great deal that still needs to be done.

This report is organized into five topical areas:

- The role of the USCG and extending physical security to cyber security -  cyber risk management
- Organizational systems for information sharing
- Motivation and barriers for sharing information
- What information to share, and what to share rapidly vs. slowly

- Technologies to support information sharing

***A Comment on Terminology***: In this paper, we use the terms “cyber security” and “cyber risk management” somewhat interchangeably. We tend to favor the latter terminology since we feel that management of cyber risk is a key to maximizing cyber security.

## 3. Context

In the maritime cyber security arena one may identify five kinds of adversarial threats or risks. One is TCOs (Transnational Criminal Organizations) which might disrupt cyber systems with goals such as hijacking, concealing contraband transport, or, potentially, hostage-taking. A second class of threats would originate with Violent Non-State Actors (VNSA) such as Al Qaida or ISIS/ISIL. While these might exploit some of the same technologies, they may have goals quite different from the essentially economic goals of TCOs[1]. Maritime cyber-systems are subject to attack by nation-states, either as part of a declared war, or part of an undeclared military contact, such as the encounters in the South China Sea. So-called “hacktivists,” cyber specialists acting in extreme ways in support of a cause, may create havoc and cause damage to call attention to a social or political issue. Finally, there may be cyber attacks for purposes of corporate espionage. For each of these, the response requirements, both in terms of velocity, and of appropriate responding agents, may be quite different. And this, in turn will affect the architecture and technology, as well as the legal structure for information sharing. It should be emphasized that careless cyber behavior or misuse of cyber systems is a major cause of cyber system failures with potential consequences as serious as those of deliberate attacks, and information sharing abut the consequences of such behavior or misuse is also covered by our findings and recommendations.

### 3.1.Maritime Cyber Risk Management a Novel Challenge

The problem of information sharing for maritime cyber risk management has little in common with many marine security issues. Because of this, there are not strong analogies. One key issue of maritime safety and security is hull breach. The defense is waterproof bulkheads. But the analogous approach – shutting off cyber communications, removes their value completely. Whether the cyber system is GPS, or other computer controlled systems, their key contribution to maritime activity is their ability to bridge long distances, and maintain nearly instant situational awareness. Therefore nothing analogous to a “complete lockdown” seems feasible. As to the cause of hull breach, other than rare failures due to extreme weather, and those due to poor maintenance, the key cause is obstructions, which are more or less fixed in space. In contrast, cyberspace does not offer “chartable hazards,” as bad actors can rapidly change their IP addresses or obscure them completely. The closest analogy to physical world hazards seems to be the notion of a “campaign,” in which similarities in the specific technologies and messages serve to “locate” an attack in some abstract “ocean of possible attacks.” Assembling information in terms of those characteristics seems to come closest to the historical approaches to maritime safety and security. Whether that abstract ocean of threats can be usefully presented remains to be explored.

[1] http://www.sanctionswiki.org/TCO

## 3.2.Layers of Interaction

The problem of organizing for maritime cyber risk management seems to have three distinct aspects that must be considered. These arise because the players are of very different types: governments and their agencies, commercial shipping and cruise firms, the onboard captains and crew and the ports and associated personnel. Their coordinated efforts to advance Maritime Cyber Risk Management appear to involve at least three different "layers" of concern: communications and technology arrangements, economic considerations, and legal and regulatory matters.

### Communication and Technology Arrangements

In the **communication and technology layer**, we find the problems of collecting information (about attacks and signatures) and of distributing warnings and remedies. The key considerations for this layer are of two kinds: technical capability, and architectural design. Technical capability limits the roles that individual parties may play. Architectural design asks questions such as: what channels should be used to communicate? Is the organization peer-to-peer or centralized? How does the architecture deal with varying levels of security and classification of information? What are the trust mechanisms?

The entire MTS comprises many players with outright conflicting interests, ranging from simple commercial competition to declared hostilities. How will access to shared information be limited (if at all) in consideration of these conflicts? Centralized control requires a trusted center. This can be accomplished for a single nation, but is much harder for a plurality of nations. Centralized control also puts "all the eggs in one basket" so that an attack on that control center can have widespread impact, worse than would be realized in a distributed or peer-to-peer system. There is some recent research on building decentralized systems that can enforce trust without putting all the eggs in one basket (Minsky, 1991; Minsky and Leichter, 1995; Minsky and Ungureanu, 2000).

### Economic Considerations

The **economic layer** represents not only the fact that multiple players are in competition with each other, but also the sheer costs of being a participant. Many maritime activities work on a narrow economic margin, and the costs of being an effective participant in a sharing system may be out of reach. As soon as some players are excluded, however, the entire system loses much of its value, and the outcasts are ripe for an attack that could affect many players across the maritime system. From an economic perspective every organization must watch its "bottom line." As the SONY attacks[2] showed, the entertainment industry, which had felt that cyber-security concerns were limited to IP issues, can be harmed in other ways. It has been reported that since that attack, that industry as a whole has become more interested in information sharing.

In addition to the false confidence that one will not be a target, if a firm reports that it has been hacked, it may lose the confidence of the public and suffer overall harm much greater than was caused by the specific attack. Each corporation or business is asked to weigh the potential downstream benefit to all of its competitors against its immediate loss by revealing the attack. This layer brings us face to face with all the complexities of maintaining competitive advantage when the threat is ubiquitous and invisible.

[2] Attributed to North Korea. See http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0

### Legal and Regulatory Matters

A third layer is the **legal or regulatory layer**. In the United States (and many other countries), cooperation among firms, which might have the effect of reducing competition, and therefore raising consumer costs, is tightly regulated. Since cyber risk management is a cost, and cooperation or sharing will lower those costs, such sharing is in danger of falling under the regulations. While there are proposed (limited) legislative remedies (Burr, 2015), the problem is a significant one. Conceivably there may one day be an extension of the seafarer's obligation to assist persons, to an obligation to assist systems (Davies, 2003).

## 4. The Research Process

We drew information from several kinds of sources as we compiled findings and developed recommendations for this white paper. The process is described briefly below, and was aimed to organize and synthesize the information into specific recommendations for consideration.

### 4.1.Interviews

Our best sources of information were numerous interviews with experts. We reached out to all of the participants in Working Group Team #6 of the Maritime Cyber Research Summit held at the CSU Cal Maritime Safety and Security Center, June 16-17, 2015. A summary of Working Group 6's findings and recommendations can be found in Clark and Roberts (2015). That working group focused on Information Sharing, and many of its findings and recommendations led to the topic of the present white paper. We were able to interview a majority of the Working Group 6 participants, who in turn gave us additional contacts to interview. Besides that key set of sources, we interviewed other senior USCG officers specifically charged with developing cyber risk management policies and guidelines, as well as some people in the private sector with specific expertise in areas such as maritime law and Information Sharing and Analysis Centers (ISACs), and also representatives of other government agencies such as the FBI, port security, NYPD, and other law enforcement agencies.

In all we conducted approximately thirty interviews. Most interviews were conducted by a pair of project team members who used an interview guide, took notes and later combined their notes into a single interview summary. Since we did not ask permission of the interviewees to attribute specific quotes or ideas to them, in the following, we refer to (Interviews, 2015-6) when we present a finding based on one or more interviews.

### 4.2.Literature Review

We also reviewed selected documents related to cyber risk management information sharing. Some of these are listed in the Reference section of this white paper. These include relevant legislation and regulations, government reports, security guidelines, best practices and standards, and academic research on technologies, incentives and risk related to information sharing. The documents cited in the Reference section are a tiny fraction of the literature available on this topic.

### 4.3.Port of New York and New Jersey AMSC Cyber Subcommittee

Another source of information for the project was the knowledge and experience gained from our leadership role in the Cyber Security Subcommittee of the Area Maritime Security Committee (AMSC) for the Port of New York and New Jersey. This subcommittee, formed and officially chartered in 2015, is chaired by the USCG with Rutgers University/CCICADA as a co-chair along with Stevens

Institute/Maritime Security Center and the NYPD. Meeting and working with this subcommittee brought us into contact with numerous USCG personnel, commercial partners, and representatives of law enforcement concerned with maritime cyber risk management in the region surrounding the Port of New York and New Jersey. Through meetings and conversations we were able to begin to understand issues related to cyber risk management information sharing by commercial companies (some of whom are competitors with one another), planning for cyber risk management exercises, and cyber risk management training needs. Since a primary activity of each AMSC is to create a security plan (the AMSP), a natural part of the maturation process for AMSCs is to create a subcommittee to address cyber risks. At the time of this writing, about one-third of the AMSCs have chartered cyber security subcommittees (Interviews, 2015-2016).

## 4.4.Process for Organizing and Synthesizing Information

After gathering information by conducting interviews and reading relevant documents, the project team systematically worked to organize and synthesize the information. Project team members were asked to summarize major takeaways from the interviews and literature in bullet points, and to categorize these bullet points by placing them under one (or more) of the five substantive topics under information sharing that we used to organize our project. As mentioned in Section 2, the five topics are:

- The role of the USCG and extending physical security to cyber security – cyber risk management
- Organizational systems for information sharing
- Motivation and barriers for sharing information
- What information to share, and what to share rapidly vs. slowly
- Technologies to support information sharing

These clusters of bulleted items formed the basis of the findings in Section 5 of this report. Documents and/or interviews are cited in support of the findings. The findings in turn lead to the recommendations in Section 6.

## 5. Findings

In this section, we present selected findings that provide context for the recommendations given in Section 6. Throughout this section, we link the discussion points to the recommendation(s) they produce using the notation [**R** 6.x.y] to indicate relevance to recommendation 6.x.y, for example.

## 5.1. The Role of the USCG and Extending Physical Security to Cyber Security – Cyber Risk Management

The USCG has an extensive set of guidelines and regulations for physical security. Developing cyber security – cyber risk management guidelines for the MTS seems to be a natural extension of that role for the USCG. It was suggested in interviews that the USCG could develop cyber risk management guidelines for facilities similar to 33CFR105 and continue, similarly, to develop guidelines for vessels (Interviews, 2015-6; Maritime Security, 2010). Since there are many diverse players in the MTS, and they have competing interests, these guidelines should be written at a "high" level – specifying the characteristics of a cyber risk management plan, not detailed prescriptive requirements (Interviews, 2015-6).

### 5.1.1 Resources for Planning Cyber Risk Management

There are numerous resources for planning cyber risk management, but most were not developed specifically for the maritime sector. Examples include the NIST framework (NIST, 2014), the NIST 800 series (NIST, 1990-2015), the ISO/IEC series, the Center for Internet Security Controls for Effective Cyber Defense Version 6.0, and the BIMCO recommendations (BIMCO, 2016). The ISO/IEC 27,000 series provides international best practice recommendations on security management (ISO/IEC, 2013). The Center for Internet Security (CIS) Controls for Effective Cyber Defense Version 6.0 provides ways to defend against the most common and dangerous cyber attacks (CIS, 2015). The NIST 800 Series provides security guidelines, policies and procedures for federal government IT systems and organizations (NIST, 1990-2015). The BIMCO recommendations are specific to a segment of the maritime sector, and carefully address cyber security for onboard systems (BIMCO, 2016). [**R** 6.1.1, 6.1.2, 6.1.3]

The NIST guidelines are perhaps the most widely known, and provide an example framework of a process for developing cyber risk management plans (NIST, 2014), called the Cybersecurity Framework (CSF). The NIST Cybersecurity Framework was developed to support protection of critical infrastructure resources. It includes a list of steps to take (and repeat) to develop and refine a cybersecurity plan. Additionally the NIST Framework Core contains a list of "Functions, Categories, Subcategories and Informative References" that describe common cybersecurity activities. As described by NIST (NIST, 2016), "The goal of the framework is to minimize risks to the nation's critical infrastructure, such as the transportation, banking, water and energy sectors. The executive order directed NIST to work with stakeholders across the country to develop the voluntary framework based on existing cybersecurity standards, guidelines and best practices." In creating this framework, NIST was "extremely collaborative with the public sector" (NIST, 2016-2 ). However, even this framework is not a perfect document. CSF is referenced in several documents as a living document, and when requesting feedback on the framework through a response analysis, respondents felt that it needed frequent updating (suggested yearly), and that it should be done by either NIST or a neutral third party. It is important to note that CFR is "consistent with voluntary international standards" (NIST, 2015), which is important in the maritime international setting. If the USCG decides to issue guidelines for cybersecurity plan development, this could inform part of the guide.

The DHS Cyber Resilience Review (CRR) process uses the NIST guidelines. The CRR predates the NIST CFR, and although not a perfect matchup, closely aligns with the NIST framework. Included in the CRR self-assessment package is a document that maps the CRR to the CFR (DHS CRR).

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), operated through DHS, offers self-assessment tools as well. Though there are many of these tools available, the ICS-CERT Cybersecurity Evaluation Tool (CSET), is a free well supported option. DHS offers approximately 60 YouTube videos showing how to utilize this tool (CSET, 2015). CSET has several approaches for self-assessment: a questions based approach (recommended for most assessments), a standards based approach (for regulated industries, presenting requirements as they are written in the standards), and a cybersecurity framework based approach (a risk-based cybersecurity evaluation using a customized question set). This self-evaluation allows users to customize their assessment based on need: regulated industries have requirements available to assess built into the tool and there is also an option to select a desired security level (low, moderate, high, very high). Questions in the self assessment are based on 27 different categories such as access control, physical security, training, maintenance, etc., each with many subtopics.

### 5.1.2 Cyber Risk Management Audits

Guidelines that are for protocols for ports, companies, etc. should not become a basis for auditing individual approaches.  But companies may welcome government guidelines. NIST could be one such starting point (BIMCO, 2016; Interviews, 2015-6). [**R** 6.1.1]

Because cyber risk management lacks a specific physical presence, there is little functional connection, beyond physically securing (e.g., requiring two-person authentication) access points to cyber-systems. None of our interviewees discussed issues such as physical protection against GPS spoofing, and other threat-specific physical measures. Therefore, it seems that physical security and cyber risk management might be better linked through audit systems currently in place or third party audits, and companies should not rely solely on external audits (Interviews, 2015-6; BIMCO, 2016). [**R** 6.1.4, 6.1.5]

One example of audits are those performed by the Bureau of Safety and Environmental Enforcement (BSEE). BSEE regulates and inspects all oil and gas operations on the outer continental shelf (if oil rigs are in transit, they are regulated by the USCG). BSEE does not write a company's hazards plan; it is developed by the operators themselves and is approved by a third-party. BSEE assesses how well the companies meet these plans. These plans focus primarily on physical security, but in the future they may include some cyber risk management as well. It is important to note that BSEE might be a reasonable entity to conduct cyber auditing for oil and gas operations. However, as of the time of our interview, BSEE had never conducted a cyber audit.

There are additional regulations, 33CFR Subchapter H (Maritime Security, 2010), relating to maritime vessels. These regulations focus on owner/operators of Mobile Offshore Drilling Units (MODU), foreign cargo vessels greater than 100 tons, US self-propelled vessels greater than 100 tons (except commercial fishing vessels), passenger vessels with more than 150 passengers, or other types of passenger vessels carrying more than 12 passengers when including at least one passenger for hire, and certain types of barges,  tankships, and temporary assist vessels, but do not apply to warships. There are compliance audits for various types of security and safety topics including drills and training. Audits are performed through Vessel Security Assessments, and owners or operators must have a Vessel Security Plan. This is another area to which cyber components could be added. Amendments to the Vessel Security Plans are approved  by the Marine Safety Center and may be added by the USCG or the vessel owner or operator. These regulations also apply to facilities. The regulations for facilities include access control, systems and equipment maintenance, handling cargo, training, drills and exercises required, monitoring, procedures for incidents. This is yet another area in which cyber regulations, training, drills, etc. could supplement the existing plans. Amendments to a Facilities Security Plan are approved by the Captain of the Port (COTP) and may be initiated by the COTP or the owner/operator.  [**R**.6.1.4]

Although not designed for auditing, the BIMCO guidelines may also provide suggestions for components to integrate into these cyber risk management audits, assessments, trainings, and drills.

### 5.1.3 Metrics

Our interviews made it clear that all are concerned with the cyber-threat to the MTS. However, there are not currently any agreed-upon measures in place to assess "how secure" any part of the system is.

Similarly, there are no measures in place to assess "how insecure" or "at risk" parts or subsystems may be. Clearly there is need for metrics to determine the cyber secure status of ports, vessels, container handling systems, etc. The Maritime Resource Center in Middletown, RI provides one example of an organization that is beginning to develop such metrics, through their proprietary methodology for assessing vessel and marine terminal cyber risk management. The primary use of such metrics for that organization is for use in their educational programs for mariners. However, many other uses can be envisioned, for example in cyber risk management audits. The Department of Energy's Cybersecurity Capability Maturity Model (C2M2, 2014) provides a complementary approach focused on assessing an organization's implementation and management of cyber risk management practices. Information Sharing and Communication is one of ten cyber security domains for which an organization can use C2M2 to assess the maturity of its processes. An effort to develop performance-based standards and the metrics to measure achieving those standards focused on maritime cyber risk management could be very important. [**R** 6.1.5]

### 5.1.4 Training and Exercises

The 33CFR103.515 specifies the USCG role to coordinate with the Area Maritime Security (AMS) Committee to conduct and participate in exercises to test the effectiveness of the AMS Plan. The AMS Plan should include a cyber component, and exercises should increasingly include tests of the effectiveness of the cyber risk management plan. Strategies for incentivizing sharing (together with new technologies) could be tested at upcoming or future USCG cyber risk management exercises (Interviews, 2015-6). These exercises could be held in conjunction with physical security exercises since we know a cyber attack may be brought about by physical damage or vice versa. The AMS Committee for the Port of Pittsburgh held the first such exercise in 2013. Exercises can range in scope from tabletops and workshops to full-scale, simulated, coordinated cyber attacks. In the latter case, access to a cyber range may be useful (Interviews, 2015-16). [**R** 6.1.6, 6.1.7, 6.1.8]

Conventional education (in Technical Schools, Community Colleges, Colleges and Universities) moves slowly. Today, some don't even realize that cyber is a threat (Interviews, 2015-6). It may be that the national or international coverage of dramatic problems contributes more to the essential awareness of cyber-threats than does any formal program of education. Therefore educational efforts should be of two kinds: "Slow:" the development and dissemination of courses and training materials suitable for players at all levels from port managers to mariners, and "Fast:" effective media campaigns to build upon any major attacks (or near-misses) as they occur, to increase awareness, and motivate players to engage with the training materials, and/or the sharing organizations. Building awareness and capability requires training tailored to components of the maritime system (Interviews, 2015-6; BIMCO, 2016). The private sector and non-profit organizations have an important role to play in such training (Interviews, 2015-6). This might coincide with rolling out new cyber guidance from the USCG. [**R** 6.1.9, 6.1.10]

### 5.1.5 Collaboration with Other Government Agencies

The USCG has a unique position in the MTS as part of the U.S. Government. In developing guidelines and technical standards for cyber risk management information sharing, the USCG has the opportunity to collaborate with other government agencies (such as NIST, ODNI, Cyber Command, NavSea, and DHS CERT). In support of these opportunities for enhanced information sharing, strengthened by the USCG presence at the NCCIC described below in Section 5.2, further research is needed into the most appropriate role for the USCG in (1) *pushing* best practices for cyber risk management to the private sector (versus just *posting* the information), and (2) developing regulations for sharing information about cyber attacks, vulnerabilities, and defenses with the private sector (Interviews, 2015-6). [**R** 6.1.11, 6.1.12, 6.1.13]

## 5.2.Organizational Systems for Information Sharing

The question of how to organize systems for information sharing had by far the richest source of information, as there are several model organizations, and there is a strong consensus that some combination of those models will form the basis for any effective program of cyber risk management for the MTS. Key findings seem to be that: (1) industry players, based on their resources, will play roles of varying intensity in the organizations that are developed; (2) to permit all needed kinds of cooperation some organizations should be non-governmental, while others are governmental and perhaps even multi-national; (3) issues of trade secrets, proprietary information, public embarrassment, lack of technical (IT) skills of even a basic nature, and national security will limit the willingness of players to share information, and must be countered with an array of incentives, as discussed in Section 5.3 below; (4) there are significant technical challenges in developing protocols for rapid sharing, and in coping with the expected flow of information, as participation expands to include all the parts of the MTS (see Section 5.5 below).

With such diverse organizations in the MTS, a range of organizational, technical, and incentive systems will be needed. To ensure timely dissemination to appropriate players, some of our interviewees emphasized the importance of a tiered approach to information sharing (Interviews, 2015-6). [**R** 6.2.2]

### 5.2.1. Enhancing USCG Presence at the NCCIC

Organizationally, partnering with effective national organizations can help the USCG to a running start. By increasing its presence at the NCCIC, the USCG would expand its opportunities to coordinate with NCCIC partners and report cyber risk management alerts, trends and mitigation strategies across the USCG, commercial partners, and other appropriate government agencies. We understand from interviews that the USCG currently has one member of the CG Cyber Command onsite at the NCCIC, and we are recommending this presence be extended to a 24x7 capability (Interviews, 2015-6). [**R** 6.2.1]

Through interviews and related research we learned that the NCCIC is able to receive and analyze Protected Critical Infrastucture Information (PCII),[3] a category of Sensitive but Unclassified (SBU) information that is protected from FOIA disclosure and regulatory use to encourage reporting of information important to the security of the nation's critical infrastructure. Furthermore, through the new DHS Automated Indicator Sharing (AIS)[4] program, the NCCIC is able to receive cyber threat indicators from private industry, perform automated analyses and tasks such as removing personally identifiable information (PII) or anonymizing the sender, and distribute the indicators to federal departments or private industry, as appropriate. This kind of two-way, machine to machine sharing accelerates the pace at which DHS, and therefore the NCCIC, is able to receive and provide cyber measures and signatures. Finally, the NCCIC works with a variety of DHS training and assessment tools available to Critical Infrastructure and Key Resources sectors. These tools include the previously mentioned Critical Resilience Review (CRR)[5] available as self-assessment or DHS-facilitated evaluation,

[3] https://www.dhs.gov/protected-critical-infrastructure-information-pcii-program

[4] https://www.us-cert.gov/ais

[5] https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf

and the National Cybersecurity Assessment & Technical Services (NCATS)[6] through which a variety of cyber assessment services (such as architecture reviews and red-team, blue-team penetration testing) are available at no cost to stakeholders. [**R** 6.2.1]

### 5.2.2. Re-developing the Maritime ISAC

Partnering with effective private sector organizations will be needed to bring competing firms and competing nations into an effective overall system. Relying solely on a governmental organization might limit information sharing among private sector partners (and international partners), and this leads to the idea of a re-development of the Maritime ISAC to provide an industry-focused community for information sharing (Interviews, 2015-6). [**R** 6.2.3]

Reflecting the economic layer of interaction, organizations differ in the resources they can direct to cyber risk management. Some interviewees suggested a Maritime ISAC with membership levels that provide and require different levels of information and capability (Interviews, 2015-6; FS-ISAC, 2015). A fast-acting ISAC is needed to complement periodic, face-to-face information sharing (supported by the AMSCs) since some cyber threats and attacks must be met in real time (Interviews, 2015-6). There seem to be variously: very tight agreements among small numbers of large players with major budgets (Interviews, 2015-6); more broad sharing, such as ISACS; and smaller players with low or no cyber budget or expertise. To include the full range of MTS stakeholders, some models are: ISACs; fusion centers; neighborhood watch as developed by the FBI Office in Los Angeles. Incremental development can start with key players and expand, perhaps using AMSC cyber risk management subcommittees as an initial step that the USCG is able to support immediately while industry partners evaluate the viability of developing and running an ISAC. (Interviews, 2015-6). [**R** 6.2.2, 6.2.3, 6.2.4, 6.2.7]

Reflecting both the economic and legal layers of interaction, sharing agreements may require: anonymity; authenticated messaging; and no FOIA access (FS-ISAC, 2015). The FS-ISAC model (particularly its technical systems guaranteeing submission anonymity) is a possible model for a new Maritime ISAC (FS-ISAC, 2015). [**R** 6.2.3]

Again at the legal layer, multi-national membership adds challenges. The FS-ISAC may provide a model. (FS-ISAC, 2015; Interviews, 2015-6). National laws on cyber vary greatly (Interviews, 2015-6). Since some important information is classified, it seems reasonable that a proposed Maritime ISAC ultimately be a cleared organization (Interviews, 2015-6; FS-ISAC, 2015). The ISAC could interface with other government agencies to ensure appropriate notification of organizations as part of the membership/access levels. [**R** 6.2.3, 6.2.4]

At the technical layer of interaction, shipboard systems and concerns are specialized, and, for example, legacy supervisory control and data acquisition (SCADA) systems and their network connections, in particular, need to be assessed for cyber risk (Konon, 2014). To have effective communication among those with true common interests, the ISAC or similar organization might maintain a subgroup focused on shipboard systems, perhaps guided by the BIMCO publication (BIMCO, 2016). **[R** 6.2.4]

Any industry-led information sharing platform (such as M-ISAC) and the USCG information sharing platform (such as a part of the NCCIC) must themselves share critical cyber risk management information regarding cyber threats. This leads to the idea that the M-ISAC maintain a presence at

[6] https://www.us-cert.gov/ccubedvp/federal

NCCIC, as is done by the FS-ISAC, the Aviation ISAC, the Multi-State ISAC, and others (Torres, 2015; FS-ISAC, 2015). [**R** 6.2.3]

### 5.2.3. Enhancing Cyber Incident Reporting Capability

As defined in 33CFR101.305, maritime security plans require that "activities that may result in a transportation security incident" be reported to the U.S. Coast Guard National Response Center (NRC). Some of our interviewees have suggested that the USCG either develop the capability or partner with an organization (such as the NCCIC[7]) to receive centrally information about cyber risk management incidents and suspicious activities (Interviews, 2015-6). The analysts at this organization could send relevant alerts to the affected maritime community members (Interviews, 2015-6) establishing a regulated two-way path and ensuring the USCG has all relayed information. In the mean time, we heard in interviews with port officials that there is confusion regarding whom they should contact in the event of a cyber incident (Interviews, 2015-6). The NRC maintains a hotline[8] for "anyone witnessing an oil spill, chemical relesase or maritime security incident," but there have not yet been thresholds guiding which types of incidents should be reported to the NRC (versus more locally, perhaps at an AMSC Cyber Subcommittee meeting). In fact, there are currently no regulations on reporting cyber incidents unless it reaches a Transportation Security Incident (TSI) level incident for the USCG, where TSI is defined as "any incident that results in a significant loss of life, environmental damage, transportation system disruption, or economic disruptions to a particular area."[9] No industry cyber incidents have ever reached the TSI level. We understand that the USCG Office of Port & Facility Compliance (CG-FAC) is updating its breach of security requirements soon to include thresholds for reporting (Interviews, 2015-6). [**R** 6.2.2, 6.2.8]

### 5.2.4. Enhancing AMSC Cyber Information Sharing

Currently, the AMSCs enable public and private partners in a geographic port area to meet periodically (often quarterly), discuss current concerns in the area, and build relationships of trust necessary for information sharing[10]. To maintain these relationships and extend them into cyberspace, each AMSC could follow the example of the Port of Pittsburgh AMSC, the Port of Northern California AMSC, the Port of New York and New Jersey AMSC and others and create a cyber security subcommittee (Interviews, 2015-6; Torres, 2015). As noted previously, about one-third of the AMSCs already have chartered a cyber security subcommittee. As the NY/NJ AMSC and others have done, all AMSCs could consider sharing cyber risk management information through the USCG HOMEPORT Portal (Interviews, 2015-6). [**R** 6.2.5, 6.2.6]

In many of our interviews, we were told that a large number of entities of the MTS do not have the resources to hire employees with sufficient background to understand anything beyond the most rudimentary aspects of good cyber hygiene, and certainly not information about evolving cyber attacks, cyber vulnerabilities and cyber defense. Some of these entities are represented on various AMSCs. More work is needed to understand organizational structures for information sharing that will develop ways to communicate cyber issues to the large number of MTS entities without technical expertise. [**R** 6.2.7]

[7] http://www.dhs.gov/topic/cybersecurity-information-sharing

[8] The hotline phone number can be found on the NRC homepage: http://www.nrc.uscg.mil/ Accessed 3/23/2016.

[9] http://www.uscg.mil/d8/msuBatonRouge/mtsa.asp

[10] For discussion of the importance of trust for information sharing, see: European Network and Information Security Agency (ENISA), 2010. *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*.

### 5.2.5. Multi-National Maritime Organizations: CJOS, AAPA, IMO

Complex nation-specific laws on cyber related issues along with concerns of sharing information about national security with other nations makes multi-national information sharing very challenging. “Maritime operations to counter illegal activity at sea are difficult to coordinate between nations, governing bodies, security organizations, and armed forces. Responsibilities, jurisdiction, co-ordination, information and intelligence exchange, as well as the command and control of units conducting or supporting law enforcement operations are a maze of classifications, information systems, hierarchies and varied forces. … None of the groups alone can provide all the necessary capabilities and coordination needed to succeed against threats”[11]. To help facilitate this information sharing and other security issues, the North Atlantic Treaty Organization (NATO) developed a NATO Memorandum of Understanding to create the Combined Joint Operations from the Sea (CJOS) Center of Excellence. CJOS was established on June 28, 2006, and includes 13 nations: Canada, France, Germany, Greece, Italy, the Netherlands, Norway, Portugal, Romania, Spain, Turkey, the United Kingdom, and the United States. CJOS is located in Norfolk, Virginia and is the only NATO accredited COE in the U.S. The purpose of CJOS is to “support the transformation of joint maritime expeditionary operations in assistance to NATO”[12].

The CJOS Memorandum of Understanding states that external security is the responsibility of the host nation (US) and internal security is the responsibility of the CJOS Director, following NATO and US security regulations. Relating to information sharing, the nations involved in CJOS are responsible to safeguard the security of any classified information provided in the course of the CJOS mission. Confidentiality is expected to remain intact even if the MOU is terminated or withdrawn.

CJOS held Maritime Security Conferences (MSC) from 2008-2012 which built on the idea of information sharing. In 2012 they found that “a bottom-up approach is more likely to be supported than an international governance model. … The outcome of MSC 2012 identified widespread agreement that there is a need for information sharing and, for this sharing to occur, there needs to be a shift from the current ‘need to know’ mentality to a culture of ‘need to share’”[13]. [**R** 6.2.9]

Another international maritime organization, the American Association of Port Authorities (AAPA), is a trade association representing more than 130 deep draft public ports in the United States, Canada, Latin America and the Caribbean. The AAPA provides education, services and advocacy for its members, which also include more than 300 associate and sustaining members such as inland river ports and firms doing business with corporate member ports. Some of the education opportunities available in 2015 included an intensive Marine Terminal Management Program, a Port Security Seminar and Exposition, a Cybersecurity Seminar, and a workshop on Shifting International Trade Routes. Along with the newsletters and surveys the AAPA publishes, they maintain a list of Port Industry Best Practices[14], which includes categories of resources such as Emergency Preparation Response and Recovery, that could potentially be a forum for sharing port cyber risk management guidelines. Just as BIMCO recently issued detailed Guidelines for Cyber Security Onboard Ships (BIMCO, 2016), some of our interviewees said that it might be appropriate for the AAPA to develop similarly-focused guidelines for port facility cyber risk management (Interviews, 2015-6). [**R** 6.2.10]

[11] http://www.act.nato.int/article-2013-2-14
[12] http://www.state.gov/documents/organization/75818.pdf
[13] http://www.cjoscoe.org
[14] http://www.aapa-ports.org/Issues/content.cfm?ItemNumber=1262&navItemNumber=543

The International Maritime Organization (IMO), an agency within the United Nations, has 171 member states and 3 associate members responsible for regulating shipping. The main role of the IMO "is to create a regulatory framework for the shipping industry that is fair and effective, universally adopted and universally implemented. In other words, its role is to create a level playing-field so that ship operators cannot address their financial issues by simply cutting corners and compromising on safety, security and environmental performance"[15].

In the IMO's 2014 year in review, The Maritime Safety Committee and the Facilitation Committee agreed to include on their agendas the topic of cyber security for the following year (2015)[16]. This came about after Canada presented a paper on the topic to the 39th session of the IMO facilitation committee in September of 2014. "The Canadian presentation called for voluntary guidelines on cyber-security practices to protect and enhance the resilience of electronic systems of ports, ships, marine facilities and other parts of the maritime transport system. It is understood to have suggested that cyber issues are brought into the coverage of the International Ship and Port Facility Security Code (ISPS)"[17]. The committee agreed, "recognising it as a relevant and urgent issue for the Organization, in order to guarantee the protection of the maritime transport network from cyber threats".

In a January 2016 IMO letter, describing trends affecting the organization in order to help develop their strategic framework for 2018-2023, cyber risk was at the top of the list. The following excerpt was taken from this letter: "The increasing trend in the use of cyber systems benefit the maritime industry, but their use also introduces great risk. From a security perspective cyber systems may be exposed to deliberate, malicious acts from individuals who may attempt to control, disable, or exploit cyber systems. From a safety perspective, non-targeted malware, innocent misuse of systems, and simple technical errors may impact vital systems related to ship and propulsion control, navigation-related technologies, industrial ship control technologies including propulsion, steering, ballast water management, electrical systems, heating, ventilation, air conditioning systems, cargo pumps, cargo tracking and control, ship stability control systems, fire detection and protection, gate access control and communication and monitoring systems, alarm systems and various hazardous gas alarm systems, pollution and other safety and environmental monitoring"[18]. However, the IMO does not yet publicly state what measures they will be taking.[**R** 6.2.11]

## 5.3.Motivation and Barriers for Information Sharing

The question of how to incentivize sharing among players in the MTS is a central one. As with any sharing scheme, information sharing for cyber risk management faces the "problem of the commons." Several industries appear to be further along in developing solutions, and their models provide guides. In complexity, MTS is closest to international finance, and the economic and security concerns of many kinds of organizations, and of competing nations, are involved. Positive incentives (motivations for information sharing) could include technical support and timely sharing of information or insurance

[15] http://www.imo.org/en/About/Pages/Default.aspx

[16] http://www.imo.org/en/MediaCentre/HotTopics/yearreview/Pages/2014-Security-and-facilitation.aspx

[17] http://www.allaboutshipping.co.uk/2014/10/25/imo-is-being-warned-of-scary-potential-of-maritime-cyber-attacks/

[18] http://www.imo.org/en/About/strategy/Documents/Member%20States%20-%20tdc/United%20States%20-%20Input%20to%20TDCs.pdf#search=cyber%20risk%20management

industry pressure (through rate reductions) to encourage participation. They also could include believable guarantees of protection from (1) action by competitors (2) legal action and (3) FOIA pressures by competitors, NGOs, and activist groups. Negative incentives (overcoming barriers to sharing) might include regulations and penalties for non-reporting. It may be possible to test some models in USCG exercises.

Providing incentives for sharing could be particularly important as the industry begins to take the small, initial steps that will lead to enhanced maritime cyber risk management. For example, we are recommending that the U.S. Government require "landlord" port operators[19] to incorporate maritime cyber risk management standards into the leases they issue to terminal operators for the right to use the ports. Landlord ports are highly autonomous and can easily implement requirements of this nature into their leases without waiting for a legislative or regulatory process, but terminal operators may then decide to "port shop" for easier restrictions, thereby hurting the ports working to improve cyber risk management. For this reason, regulation requiring these standards at all ports is needed to ensure a "level playing field" in cyber risk management, preventing terminal operators from being able to avoid cyber standards by relocating to a more "lax" port operator (Interviews, 2015-6). [**R** 6.3.1]

Realization of this kind of legislation or regulation will likely take some time, however, and in the interval, there are opportunities to motivate early adoption of enhanced cyber risk management practices. As port operators negotiate leases with tenants, they could, for example, offer discounted rates to tenants that agree to comply with cyber risk management standards (Interviews, 2015-6). Futhermore, the terms of port leases could be opportunities for requiring tenants' participation in a reinstantiated M-ISAC. [**R** 6.3.1, 6.3.2, 6.3.3]

Players in this industry bring greatly different resources to the problem (Interviews, 2015-6). The arrangements made at the E-ISAC (Electrical Industry) and the FS-ISAC (Financial) may yield useful models for development of incentives (Interviews, 2015-6; FS-ISAC, 2015). We heard in interviews, for example, that the FS-ISAC maintains a Gmail Listserv for communicating threat information to its members, and the fact that U.S. Law Enforcement is not allowed to join the list encourages foreign-based partners to participate (Interviews, 2015-6). Other models are the FBI, which shares at industry conferences, and the Oil and Gas industries (ONG-ISAC) (Interviews, 2015-6; FS-ISAC, 2015). It seems clear that incentives will have to be tailored to be effective for the various classes of players. [**R** 6.3.4, 6.3.5, 6.3.6]

Since information sharing benefits all, but costs the contributors, distillers and disseminators, there is a risk of "free-riding" (Gal-Or & Ghose, 2005). However, the MTS is an interdependent system of systems, and a major cyber event somewhere in the system will likely disrupt the business of all parties and potentially affect the reputation of the whole industry (Interviews, 2015-6). [**R** 6.3.5]

Some useful incentive models may be found in other domains, such as the WHO's provision of subsidized vaccine targeted to countries reporting outbreaks of bacterial meningitis (Laxminarayan, et al., 2014). It is possible that compliance in sharing will be motivated by the insurance industry, although it has not yet taken any positions on this issue (Interviews, 2015-6). [**R** 6.3.6]

[19] See the American Association of Port Authorities (AAPA) Glossary of Maritime Terms for definitions of "landlord" vs. "operating" ports. http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1077 Accessed 3/23/2016.

The European Network and Information Security Agency (ENISA) found, in a research effort regarding information sharing for network and information security, that stakeholders felt “Economic incentives stemming from cost savings” were of the highest importance for information sharing, whereas “Economic incentives from the provision of subsidies” or “Economic incentives stemming from the use of cyber insurance” were of low importance (ENISA, 2010). That is, the participants identified the most important incentive for participating in an Information Exchange (IE) such as an ISAC to be the cost savings they would realize from more efficiently allocating the information security resources of the group. The challenge remains, however, to prove that participation in an IE does bring these savings and efficiencies (ENISA, 2010). [**R** 6.3.6]

A different kind of incentive for information sharing, ranked third in importance out of ten incentives for information sharing by the participants in the ENISA research Delphi exercise, is the “presence of trust amongst IE participants”. Although trust is perhaps more difficult to quantify than cost savings, many interviewees highlighted operating and sharing information within a community of trusted partners (such as the current AMSCs) to be a critical component of the current security arrangements (Interviews, 2015-6). Furthermore, a 2001 study of organizations accustomed to sharing information, conducted by by the U.S. General Accounting Office (GAO), found, “All of the organizations identified trust as the essential underlying element to successful relationships and said that trust could be built only over time and, primarily, through personal relationships” (U.S. GAO, 2001). [**R** 6.3.6]

## 5.4.What Information to Share, and What to Share Rapidly vs. Slowly

What information should be shared? The Cybersecurity Information Sharing Act of 2015 (Burr, 2015) proposes requirements for communication of “cyber threat indicators,” defining these as the “information necessary to describe or identify.” The Act identifies eight categories of cyber threats, and could be the framework of a strategy describing what to share regarding threats. More broadly, the FS-ISAC structures its sharing according to incidents, threats, vulnerabilities, and resolutions/solutions (FS-ISAC, 2015). We learned that information shared with the MS-ISAC may include: advisory notices, tactical information, and known malicious IPs (Interviews, 2015-6). Information to share will include: vulnerabilities, TAXii[20] information, botnet information, malicious IP addresses, near misses, incidents, threats, resolutions/solutions, and the seven key Netflow fields (Interviews, 2015-6). Once again the economic layer is in play here as only a select set of private sector companies and law enforcement agencies have the resources to dedicate groups of highly skilled people to analyze this information. [**R** 6.4.1]

A Red|Yellow|Green Traffic light protocol to code sensitivity of information could be useful (Interviews, 2015-6; FS-ISAC, 2015; BIMCO, 2016). [**R** 6.4.2] The Port of NY and NJ has developed what many regard as a “best practice” for sharing sensitive but unclassified information with private sector partners (Interviews, 2015-6). The process involves individual invitations to a closed door meeting where participants’ identification are checked at the door. Participants are typically long-standing AMSC members, and the meeting is chaired by the COTP. If further dissemination of information beyond the meeting is deemed necessary, the USCG vets the information to remove the sensitive material. This process may include a USCG legal advisor if necessary. Once fully vetted, the information is posted to the HOMEPORT portal.

[20] **https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-**with-standardizing-threat-information/

Targeted small briefings, including classified briefings, are vital, but these typically lag events by weeks. Faster sharing is needed. "Slow" sharing can also be done at industry conferences or with AMSCs (Interviews, 2015-6). Research may be needed to automate the filtering and classification of the large volume of information (Interviews, 2015-6). Additional research is needed into the cyber risk management industry issue of filtering the large volume of information available on cyber incidents. More information is not always better, and it can be difficult to filter through the noise to understand what is actually a malicious attack. Key players need to avoid information overload, which can cause actual events to be overlooked as noise. This is not just a maritime cyber issue, but a cyber risk management industry issue in general. [**R** 6.4.2, 6.4.4]

Because information about potentially catastrophic near misses may unduly influence cyber risk management investment decisions (Dillon & Tinsley, 2015), one can ask whether these events should be examined to determine whether resilience was key to the "miss." This could help others to learn from the disseminated information. [**R** 6.4.3]

## 5.5.Technologies to Support Information Sharing

Technology presents several challenges: Each player must have adequate resources to share and receive information, to protect sensitive information, and to respond promptly enough. The players have to agree on protocols for reporting problems, attacks, and countermeasures. The responsible coordinating bodies must also have technologies for receiving and filtering streams of information, prioritizing them, and classifying them for controlled dissemination to the players.

Rapid sharing requires standardized reporting, etc. The FS-ISAC employs the STIX and TAXii systems that are being developed by a community led by DHS. STIX and TAXii may be relevant for standardized reporting, but they are not software tools. Full implementation should not require vendor specific software (FS-ISAC, 2015-6; Interviews, 2015-6). Several existing protocols/systems could be evaluated to see whether they are appropriate for MTS use (Interviews, 2015-6). For example, the FS-ISAC uses technical systems developed by Soltra, a DTCC and FS-ISAC company. The systems include a threat intel server, SoltraEdge, to aggregate and distribute information about threats (peer-to-peer and firm-to-firm) and the SoltraNetwork that connects these servers in a hub and spoke manner. [**R** 6.5.1. 6.5.3]

Utilizing STIX and TAXii is the new DHS Automated Indicator Sharing (AIS)[21] program. As previously mentioned, this is now used by the NCCIC. AIS is a two-way sharing program, which does not need a human in the loop to share information; the information is shared from machine-to-machine, either from the NCCIC to partners or from partners/industry to the NCCIC.

The National Cybersecurity Protection System (NCPS) is a system of systems providing capabilities to defend the federal government's information technology infrastructure. NCPS broad cyber security capabilities include detection, analytics, information sharing, and prevention. For example, its analytics capabilities include Secure Information and Event Management (SIEM), Packet Capture (PCAP), Enhanced Analytical Database (EADB) and flow visualization, and Advanced Malware Analysis. These or related technologies may prove useful in developing information to share within certain segments of the MTS.

[21] https://www.us-cert.gov/ais

The ability to anonymously submit reports of cyber risk incidents or near misses could allow firms to share information without fears of harming their reputations or incurring regulatory penalties. An example of this kind of anonymized incident reporting is found in the collaboration of the American Bureau of Shipping (ABS) and Lamar University to develop and maintain an online Mariner Personal Safety (MPS) database[22] for tracking maritime injury and close call reports (Interviews, 2015-6). Another example of data anonymization is the Vocabulary for Event Reporting and Incident Sharing (VERIS) framework[23] used by Verizon to gather information for its annual Data Breach Investigation Report. Finally, the FS-ISAC has as one of its Cornerstones that information is able to be submitted anonymously through its technical systems (FS-ISAC, 2015). The M-ISAC or other consortium of MTS partners could increase participation in information sharing by identifying or developing an independent data anonymization platform for sharing cyber risk management incidents and false alarms (Interviews, 2015-6). [**R** 6.5.4]

Recent research in decentralized "trust systems" also may prove helpful (Minsky, 1991; Minsky and Leichter, 1995; Minsky and Ungureanu, 2000). [**R** 6.5.2]

# 6. Recommendations

## 6.1. The Role of the USCG and Extending Physical Security to Cyber Security – Cyber Risk Management

6.1.1. We strongly endorse the ongoing USCG effort to develop cyber risk management guidelines analogous to the physical security requirements found in 33CFR Subchapter H.

6.1.2. Since there many diverse players in the MTS, and they have competing interests, we recommend guidelines for the MTS be written at a "high" level – specifying the characteristics of a cyber risk management plan, not detailed technical prescriptions.

6.1.3. We recommend the NIST Framework (NIST, 2014) as a guide for the process of developing cyber risk management plans covering facilities, NIST (1990-2015) as a resource for federal government IT system security, and BIMCO (2016) as a resource for developing cyber risk management guidelines specific to vessels.

6.1.4. We recommend that physical security and cyber risk management be more strongly linked, reflecting the likelihood that a cyber attack may be manifest by physical damage or vice versa. This may be facilitated through the audit systems currently in place, such as found in 33CFR Subchapter H (Maritime Security, 2010), in addition to self-audits. These may also be integrated into current vessel and facility drills, exercises, and trainings. The BIMCO Guidelines may offer some insight of topics to include.

6.1.5. We recommend a research effort to develop cyber risk management performance-based standards and metrics to be used by the USCG in security audits, educational programs, and other

[22] http://ww2.eagle.org/en/rules-and-resources/safety-human-factors-in-design/mariner-personal-safety.html Accessed 3/24/2016

[23] http://veriscommunity.net/index.html Accessed 3/21/2016

applications. Again, these can be added as additional content into pre-existing vessel and facility drills, exercises, and training.

6.1.6. We recommend the USCG develop and roll out the capability to assess and communicate the cyber readiness of the MTS and its components.

6.1.7. We recommend that the USCG increase its effort to coordinate and lead regular cyber risk management exercises in collaboration with the AMSCs and in conjunction with phycial security exercises. Exercises should range in scope and complexity as appropriate from tabletops to full-scale simulated cyber attacks perhaps facilitated by access to a cyber range.

6.1.8. We recommend cyber risk management exercises as opportunities for evaluating proposed organizational structures, performance-based standards and technologies for information sharing within the USCG, and between the USCG, its commercial partners, and other government agencies.

6.1.9. We strongly endorse ongoing USCG efforts to provide guidelines for training to raise awareness of cyber risk management threats for members of the AMSCs. Considerations such as who pays for the training and who develops, delivers and receives the training need to be worked out.

6.1.10. We recommend cyber risk management training tailored to specific components of the maritime system be developed to coincide with, and enhance understanding of, new cyber guidance from the USCG.

6.1.11. We recommend that the USCG expand collaboration with other government agencies (such as NIST, ODNI, Cyber Command, NavSea, and DHS CERT) to develop technical standards for cyber risk management information sharing.

6.1.12. We recommend further research into the appropriate role of the USCG in pushing best practices for cyber risk management to the private sector.

6.1.13. We recommend further research into the appropriate role of the USCG in developing regulations for sharing information about cyber attacks, vulnerabilities, and defenses with the private sector.

## 6.2.Organizational Systems for Information Sharing

6.2.1. We recommend the USCG enhance its presence at the NCCIC into a 24x7 capability for coordinating with NCCIC partners and reporting cyber risk management alerts, trends and mitigation strategies to the USCG, commercial partners, and other appropriate government agencies.

6.2.2. We recommend that the USCG lead an organization (such as a branch of the NCCIC) for sharing cyber risk information with its MTS partners, which may include several tiers of information corresponding to the type of information to be shared (automated reports of probes vs. discussion of possible trends over time, etc.) with appropriate groups of partners such as ISACs, fusion centers, AMSCs, local FBI offices, and state and municipal law enforcement units. We note that not all MTS partners will be able to participate at all levels of sharing (limitations may be technical, economic, or based on national policy).

6.2.3 We recommend that private industry within the MTS develop and lead an industry-focused organization (such as a re-instantiated M-ISAC) for sharing cyber risk information, providing an arms-length relation to the USCG-led organization in Recommendation 6.2.1. Investigation of the business and technical models employed by existing organizations such as the FS-ISAC, E-ISAC, ONG-ISAC, and A-ISAC, particularly as relates to supporting anonymous sharing of information, may provide a good starting point for this organization.

6.2.4. We recommend that the industry leaders of the M-ISAC establish membership levels that vary according to the member's size (ability to contribute financially) and industry sector (terminal operator, oil and gas import/export, international shipping, etc.).

6.2.5. We strongly endorse the requirement, proposed in the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015 (Torres, 2015), that each AMSC create a cyber risk management working group or subcommittee, and we recommend the subcommittee meet at least quarterly.

6.2.6. We recommend a system-wide coordination effort to develop a compilation of mission, focus, and operation found at existing AMSC cyber security subcommittees, with results to be shared across AMSCs.

6.2.7. We recommend further research on the best organizational structures for sharing information with components of the MTS that do not have any information-technology-trained personnel.

6.2.8. We recommend that all MTS partners report cyber security incidents, including near misses, to the USCG National Response Center (NRC) until an alternative organization (perhaps the NCCIC) is identified and reporting requirements are specified in the cyber risk management guidelines referred to in Recommendation 6.1.1.

6.2.9. As found by CJOS, "a bottom-up approach is more likely to be supported than an international governance model". We recommend this approach be utilized, emphasizing buy-in from international industry partners as much as possible rather than regulations.

6.2.10. We recommend the American Association of Port Authorities (AAPA) develop cyber risk management guidelines for port facilities, similar to the BIMCO (2016) guidelines for ships.

6.2.11 We recommend that the USCG continue to work with the IMO and monitor their international efforts to establish cyber risk management guidelines.

### 6.3. Motivation and Barriers for Information Sharing

6.3.1. We recommend that the USCG advise Congress that legislation and/or regulation is needed that requires "landlord" port operators to incorporate maritime risk management standards in their leases to terminal operators and "operating" ports to adopt the standards themselves.

6.3.2. We recommend that "landlord" port operators offer discounts to terminal operators that agree to adopt cyber risk management standards before legislation requires it.

6.3.3. We recommend that "landlord" port operators require their tenants to be members of the M-ISAC once it is reinstantiated.

6.3.4. We recommend that the new M-ISAC communicate threat information among its membership in a way that does not involve the U.S. Government or Law Enforcement in order to encourage participation by non-U.S. firms. We note that U.S. firms may be required to also (separately) report threat or incident information to an appropriate U.S. authority.

6.3.4. We recommend that industry partners working to establish new information sharing agreements evaluate the incentives used to avoid pitfalls such as free-riding and withholding critical information from competitors in the FS-ISAC, ONG-ISAC and E-ISAC.

6.3.5. We recommend research efforts focused on the following:

6.3.5.1: In-depth interviews with all participants in an AMSC to identify the specific barriers to investment in information sharing faced by these MTS partners. Incentive plans, such as identification of a third-party anonymization service for reporting incidents, can then be proposed to target these specific, MTS-centric barriers.

6.3.5.2: The legal challenges of global cyber risk management information sharing and incentives.

6.3.5.3: Methods to achieve rapid and useful information sharing in a way that both large and small players in the MTS can participate, and in particular on how one can entice larger content providers to take the lead on information sharing.

## 6.4.What Information to Share, and What to Share Rapidly vs. Slowly

6.4.1. We recommend that categories of information to be shared could be taken from existing sources that include: the TAXII, STIX and CybOX specifications[24], the FS-ISAC categories of information for submission (Incidents, Threats, Vulnerabilities, and Resolutions/Solutions), the threat types listed in CISA 2015, and data elements known to be shared by MTS entities with organizations such as the MS-ISAC.

6.4.2. We recommend development of standardized protocols for managing the sensitivity (as relates to confidentiality and to timing) of information to be shared. Examples of protocols in use that could serve as models are the USCG RGA (Red, Green, Amber) scheme, and the approach employed at the Port of NY/NJ.

6.4.3. We recommend that reports of “near misses” be shared together with an analysis of the apparent reason(s) the attack was unsuccessful.

6.4.4. We recommend additional research into the cyber risk management industry issue of filtering the large volume of information available on cyber incidents (noise vs. malicious). More information is not always better; instead, the research should focus on what is the most important critical information that key players need to avoid information overload, which can cause actual events to be overlooked as noise. Additionally, different MTS partner organizations, and different roles, positions, and levels within these organizations, will require different kinds of filters to ensure the right information reaches each party.

## 6.5.Technologies to Support Information Sharing

6.5.1. We recommend research to evaluate how existing technical protocols for information sharing (such as TAXii/STIX) are currently at use by MTS partners, such as the MS-ISAC, and how their use could

[24] https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

be more widely adopted where needed. Rather than identify products from a single vendor, technical recommendations should identify industry protocols supported by multiple software products.

6.5.2. All of the models discussed so far have one or two central nodes, which present a single point of failure (SPOF). We recommend further research seeking distributed models that can deal with the complexities of the MTS without presenting a SPOF.

6.5.3. We recommend a research effort aimed at analyzing the many vehicles for sharing to see what role they may play in a comprehensive information sharing strategy for the MTS. Examples include: HOMEPORT, sharepoint, briefings (internal, other agencies, etc.), DHS Communities of Practice, forums, and automated network monitoring systems.

6.5.4. We recommend that the MTS industry research available anonymization platforms and technologies that could allow commercial partners to share cyber risk information such as incidents and false alarms without fear of negative publicity. Examples include: the online Mariner Personal Safety (MPS) database led by American Bureau of Shipping and Lamar University, the Vocabulary for Event Reporting and Incident Sharing (VERIS) framework[25] used by Verizon to gather information for its annual Data Breach Investigation Report, and the technical systems used by the FS-ISAC to allow anonymous submission of threat information by its members.

## 7. References Cited

BIMCO, 2016. The Guidelines on Cyber Security Onboard Ships. URL https://www.bimco.org/~/media/Products/Manuals-Pamphlets/Cyber_security_guidelines_for_ships/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016.ashx (accessed 1.12.16)

Burr, R., 2015. S.754 - 114th Congress (2015-2016): Cybersecurity Information Sharing Act of 2015 [WWW Document]. URL https://www.congress.gov/bill/114th-congress/senate-bill/754 (accessed 12.19.15).

C2M2, 2014. Cybersecurity Capability Maturity Model, Version 1.1. Department of Energy, February, 2014. URL http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf (accessed 2.15.16)

CIS, 2015. CIS Critical Controls for Effective Cyber Defense Version 6.0. Center for Internet Security. URL http://www.cisecurity.org/critical-controls.cfm

Clark, B.G., and Roberts, F., Summary Report of Findings: Maritime Cyber Security Research Summit, July 2015.

[25] http://veriscommunity.net/index.html Accessed 3/21/2016

CSET Cybersecurity Evaluation Tool, 2015. YouTube Video Tutorial: 13 CSET 6.2 Questions Screen. URL https://www.youtube.com/watch?v=CfRDUqA5WnI

Davies, M., 2003. Obligations and Implications for Ships Encountering Persons in Need of Assistance at Sea. Pac Rim Pol J 12, 109.

Department of Homeland Security (DHS). Cyber Resilience Review. URL https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf

Dillon, R., Tinsley, C., Near-Misses and Decision Making Under Uncertainty in the Context of Cybersecurity. Ed. Book, Improving Homeland Security Decisions, forthcoming.

European Network and Information Security Agency (ENISA), 2010. Incentives and Challenges for Information Sharing in the Context of Network and Information Security.

Financial Services Information Sharing & Analysis Center (FS-ISAC), 2015. Operating Rules. URL https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_2015.pdf (accessed 1.12.16).

Gal-Or, E., Ghose, A., 2005. The Economic Incentives for Sharing Security Information. Information Systems Research 16(2), 186-208.

Interviews, 2015-6. Interviews with Industry and Other Experts, Conducted by CCICADA.

ISO/IEC, 2013. International Organization for Standardization, ISO/IEC 27001 – Information Security Management.

Konon, J., 2014. Control System Cybersecurity: Legacy systems are vulnerable to modern-day attacks. Proceedings of the Marine Satefy & Security Council, the Coast Guard Journal of Safety at Sea 71(4), 45-47.

Laxminarayan, R., Reif, J., Malani, A., 2014. Incentives for Reporting Disease Outbreaks. URL http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0090290. (accessed January 12, 2016).

Maritime Security, 33CFR Subchapter H pt. 101-107 (2010). URL https://www.gpo.gov/fdsys/granule/CFR-2010-title33-vol1/CFR-2010-title33-vol1-part101 (accessed 1.12.16).

Minsky, N.H., 1991. The imposition of protocols over open distributed systems. Softw. Eng. IEEE Trans. On 17, 183–195.

Minsky, N.H., Leichter, J., 1995. Law-governed Linda as a coordination model. Springer.

Minsky, N.H., Ungureanu, V., 2000. Law-governed interaction: a coordination and control mechanism for heterogeneous distributed systems. ACM Trans. Softw. Eng. Methodol. TOSEM 9, 273–305.

National Institute for Standards and Technology (NIST), 1990-2015. Special Publications SP-800 Computer Security. URL http://csrc.nist.gov/publications/PubsSPs.html#SP%20800

National Institute for Standards and Technology (NIST), 2014. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. URL http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (accessed 1.12.16)

National Institute for Standards and Technology, 2015. Overview of the Cybersecurity Framework. URL http://www.nist.gov/cyberframework/upload/cybersecurity_framework_coast_guard_maritime_public_meeting_2015-01-15.pdf

National Institute for Standards and Technology (NIST), 2016. Cybersecurity Framework Comments Reveal Views on a Framework Update, Increased Need to Share Best Practices and Expand Awareness. URL http://www.nist.gov/itl/acd/cybersecurity-framework-comments-reveal-views-on-a-framework-update.cfm

National Institute for Standards and Technology, 2016-2. Analysis of Cybersecurity Framework RFI Responses. URL http://www.nist.gov/cyberframework/upload/RFI3_Response_Analysis_final.pdf

Torres, N., 2015. H.R. 3878 – 114th Congress (2015-2016): Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015. URL https://www.congress.gov/bill/114th-congress/house-bill/3878/text (accessed 1.12.16).

United States General Accounting Office (U.S. GAO), 2001. Information Sharing. Practices that can benefit critical infrastructure protection. Washington, D.C.