AAPA American Association of Port Authorities

Alliance of the Ports of Canada, the Caribbean, Latin America and the United States

Seaports Deliver Prosperity

September 11, 2017

R.D. Manning
Captain
U.S. Coast Guard
Chief, Office of Port and Facility Compliance
2703 Martin Luther King Jr. Ave
Washington, DC 20593-7501

AAPA Comments to Docket No. USCG-2016-1084 – Draft Navigation and Vessel Inspection Circular (NVIC) 05-17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities

Dear Captain Manning:

On behalf of the American Association of Port Authorities (AAPA), I would like to extend our gratitude for the opportunity to provide input into the guidelines for addressing cyber risks at Maritime Transportation Security Act (MTSA) regulated facilities. Our members appreciate that operators may use this document as a benchmark to develop and implement measures and activities for effective self-governance of cyber risks.

AAPA is the unified and collective voice of the seaport industry in the Americas. AAPA empowers port authorities, maritime industry partners and service providers to serve their global customers and create economic and social value for their communities. Our activities, resources and partnerships connect, inform and unify seaport leaders and maritime professionals in all segments of the industry around the western hemisphere. These comments are on behalf of our U.S. members.

Today, international trade through seaports accounts for over a quarter of the U.S. economy – and is projected to reach 60 percent by 2030. At the center of trade and transportation are America's seaports, which handle approximately $6 billion worth of import and export goods daily, generate over 23 million American jobs, and generate $321 billion in tax revenues. Security is a top priority for AAPA members, be it physical or cyber, due to the direct impact ports have on the safety of our communities and on our nation's economic supply chain.

Strategically, commercially regulated port facilities have a long history and common understanding on how the U.S. Coast Guard (USCG) can change security postures given emerging threat levels across a port environment. For example, ports firmly understand that MTSA regulations are designed to provide the general parameters for port and facility security, while allowing facility owners and operators the discretion to determine the details of how they will comply. The result is that the owners and operators are responsible for assessing vulnerabilities and ensuring the security of their facilities with USCG oversight and guidance.

However, our members also understand that commercial port partners also embrace the capabilities an Armed Service and law enforcement entity can bring to bear to defend and protect the maritime environment in and around ports. The Coast Guard has clear specifications on how a Maritime Security (MARSEC) Level could change and what physical response actions by the public and private sector are needed. There is nothing in the MARSEC requirements that provide increasing levels of cyber defense for the government or private sector, yet a cyber event could cause physical world impacts.

Addressing cyber risks is an evolving partnership with terminal operators, port and transportation stakeholders and USCG. Where this NVIC and Coast Guard industry engagement is silent is on the level of security and response USCG will provide the industry in the event of a change to the maritime security level related to a transportation security incident triggered by a cyber event. More definition and clarity is necessary for ports as it factors into risk-based decisions on how to operate our facilities as maritime security levels change in the port or offshore environment.

Historically, when USCG engages with the maritime industry regarding vessel navigation, safety and security, as well as environmental protection, USCG often provides training and exercises to facilitate industry understanding of new standards and technology. With the release of NVIC 05-17, it is still unclear how USCG maritime inspectors and security specialists should engage with facilities, and what standards they will use to approve cybersecurity vulnerability assessments, security plans, as well as the appropriate level of understanding by facility security officers. Without clear engagement with ports and a basic understanding, industry will have a hard time providing USCG with a consistent security posture across either local or national maritime security environments. AAPA recommends that USCG commit to providing training and exercises, so both the inspectors and the ports have a better understanding on how to respond.

The highest risk to maritime facilities comes from failure of onboard safety mechanisms that would automate quick response in the event of a Transportation Security Incident (TSI). These marine safety systems are trusted and relied upon by both the industry and the operators. In each new release of these marine safety systems, they relate to more sophisticated digital systems, yet there is no guidance on monitoring or security in these “Internet of Things” (IoT) devices. The Coast Guard already regulates safety devices on vessels and platforms regarding physical capabilities of devices, such as currency of flares and life rafts, feasibility of fire suppression systems, etc. Cybersecurity guidance and/or inspection of marine safety systems would go far to reduce the risk of injury, environmental damage or loss due to system loss, and compromise or damage due to a cybersecurity breach.

Every organization, industry and government faces cyber threats, and none of us are immune to their disruptive potential. AAPA appreciates government partners in the fight against organized criminal gangs, hacktivists and state-sponsored attacks. Our members welcome the opportunity to work with USCG to craft guidelines that would enhance current security measures and information sharing practices between government and the maritime community and reflect the conditions of an increasingly digital world. We appreciate your consideration of our concerns and look forward to working with you to develop guidelines for a more secure and safe maritime environment.

Attached are additional recommendations to the NVIC provided by individual AAPA members and specifically from members of the Security Committee and IT Committee.

Security is a top priority for AAPA and its members. We stand ready to work closely with the Coast Guard to develop improvements to cybersecurity issues and protocol that clearly articulate the various roles and requirements to ensure we address this growing threat to our economy. If you have any further questions, please do not hesitate to contact me directly

Sincerely,

Kurt J Nagle

Kurt J. Nagle
President & CEO
American Association of Port Authorities

ATTACHMENT

Below are individual comments received from AAPA members.

GENERAL COMMENTS

1. *Industry and Government Expertise.* Throughout, the document guidance refers to broad terms for responsible industry parties, as well as cybersecurity tools. In the best case, the government must recognize that small but essential maritime facilities and port partners may not have multiple levels of management as described in the document. In addition, the guidance references deploying an automated asset inventory discovery tool and a file integrity checking analysis tool. We request more clear guidance as to how Coast Guard Marine Inspectors are trained to understand titles of maritime and port facility roles and cybersecurity tools, as well as reconcile the security they may provide maritime facilities.

   The MTSA provides a very good framework to aid facilities in establishing useful, relevant and workable Security Plans. However, critical to the success of any Security Plan is the close coordination with law enforcement, intelligence and regulatory agencies on emerging, reliable information as early as possible in the security cycle. This coordination requires access by Company Security Officers (CSO) and Port/Facility Security Officers (PSO and FSO) to information that is classified. Without clarity on the clearance process, CSOs, PSOs and FSOs are often left to retrieve information from the same sources as the general public and on the same timeline as the general public. This significantly hampers the ability of officers to effectively manage their responsibilities and adequately protect people, operations and property. Some reference to the appropriate clearance application procedures in the MTSA regulations could help fill this void. Whatever industry can do to support further understanding in this area, we stand ready to provide it.
2. *Page Numbering.* Please number pages by enclosure, 2-1, etc., to preserve traditional NVIC formatting.

ENCLOSURE 1

1. *(p. 2-5) Specific Enclosure 1 Section Guidance:* There is a lack of clarity concerning the purpose of the regulatory sections and the italicized text below each section. The explanation in the NVIC: "Depending on the results of the FSA, this section contains portions of subchapter H that may be applicable. The italicized text provides general, recommended guidance on how to mitigate cyber vulnerabilities determined during the FSA." We interpret this to mean that if the FSA shows deficiencies in any of these regulatory areas that involve cyber, these pages give guidance on how cyber should be addressed in each section. Industry requests more clarity on the application of cybersecurity in these subsequent sections.
   a. A characteristic of the document that occurred to me, as FSO of a small facility, is the difficulty in application to smaller facilities. The NVIC doesn't apply to only larger facilities, or only facilities with a MSRAM score of "x", but to all 105 and 106 facilities. Enclosure 2 is "How to Apply the NIST CSF to the MTSA World." In my opinion, it does an excellent job of explaining that application to larger facilities, and we have sure needed that explanation! But the MTSA world is wide indeed, encompassing small facilities with big risk and large facilities with lower risk. The NVIC, like Subchapter H, should be flexible enough to fit them all. The language used doesn't seem to envision or include smaller facilities. Below are some examples.
      i. Establishing Cyber Risk Management. Concepts that are mentioned that refer to larger organizations include "senior management," "all levels of an organization," "highest level in the organization and with appropriate intermediate management levels". The ideal risk management team on p. 3 is a team from a large facility or a port authority. What does the Coast Guard envision that this team looks like at a small facility of 20-50 employees? Less than 20?
      ii. Create a Cyber Risk Management Program. "One common practice to mitigate the difficulty of managing cybersecurity within large/complex organizations is to appoint an owner for each IT/OT asset, who then becomes responsible for its day-to-day protection." Small organizations also find it difficult to manage cybersecurity.
      iii. Enterprise Wide Inventory and Analysis. "Deploy an automated asset inventory discovery tool." Will a smaller facility be able to locate and deploy this tool? If I ask my petty officer inspector about such a tool, how is he/she going to respond? This comment also applies to "file integrity checking tools." Any term that more than 50 percent of the FSO population is going to respond to with "Say what?" should probably have a short definition somewhere. Let's call this the "Say what?" rule, or link to the cyber resources section on Homeport. With that being said, we want to applaud the authors of this document for using plain standard English when the temptation to use technical language must have been nearly irresistible.

   The word "large" appears 5 times in the NVIC; and in three uses refers to large organizations or networks. The word "small" does not appear at all when used to describe organizations or networks.

   b. The NVIC gives a risk-based security assessment tool. It is a simple tool whose usefulness is demonstrated by its efficient and effective application to industries beyond maritime. This NVIC expands on the 11-02 ch. 1 process and gives several other tables (Appendix A) to use in integrating cyber into this most important portion of the assessment process. The tables and their explanation given on Enc. 2 p. 9 are readily understandable by a person without an IT background.

1. *(p. 1.) Alternative Security Program (ASP), 33 CFR 101.120:* "Owners/operators that already employ a comprehensive cybersecurity plan for their organization, or who wish to apply a standard security program that incorporates cybersecurity to multiple facilities, may wish to submit a security plan under the Alternative Security Program, 33 CFR 101.120." The Coast Guard is inviting owners/operators to utilize the ASP protocol to address one portion of their overall security program. Currently, ASPs are developed by industry groups and employed by members in good standing of these groups. ASPs address regulatory compliance holistically, without the one-to-one regulatory alignment demonstrated between the FSP and the checklist in Enc. 3 of NVIC 03-03 ch. 2. With this statement, the Coast Guard is inviting facilities to draw up individual access control, restricted area, and cargo handling sections, among others, that have nothing to do with cybersecurity.
2. *(p. 2.) Recommended Cyber Analysis as Part of the FSA:* This raises the question, is the NVIC mandating that all facilities must conduct a new FSA to incorporate cyber? Per the regulations, an FSA is performed as a precursor to the initial FSP. The FSA must be reviewed and validated, and the FSA report must be updated each time the FSP is submitted for re-approval or revisions (105.310(c)). The assessment is reviewed during the annual audit of the FSP (Enc. 8, NVIC 03-03, ch. 2). Realistically, the original FSA may not receive much maintenance between five-year re-approval cycles. It's understandable why the USCG wants to start with the FSA. That's where the plan process starts, that's where the vulnerabilities are laid out. But FSAs take time, money and personnel to perform, and facilities won't embark on them unless they have to. The NVIC states, p. 1, "Once this guidance is finalized, an owner/operator may demonstrate compliance with the regulations by including cyber risks in their FSA and including a general description of the cybersecurity measures taken in the FSP, if appropriate." Under this direction, when the final version of the NVIC is issued, it seems that all MTSA facilities will need to perform a new FSA and re-write their FSPs to include a general description of the cybersecurity measures taken to mitigate vulnerabilities. This course of action will overwhelm the inspection and approval cycle, and place a burden on smaller port and maritime facilities. Is this what Coast Guard is expecting? If it is determined that a MTSA facility is not cyber secure or has not taken cybersecurity measures as described in the NVIC, will a facility be mandated to become cyber secure?
3. *(p. 2.) Personnel Training:* The suggested language provides no actual guidance regarding cybersecurity as it relates to the noted CFR references. As an example, currently 33 CFR 105.205 describes and outlines the qualifications and responsibilities of the Facility Security Officer (FSO). Request clear delineation of the Coast Guard's expectations of FSOs.
   a. For example, is the FSO now responsible (either directly or indirectly) for cybersecurity? If so, to what extent and what are the expected qualifications? In addition, does this now mean that our IT department should be included as part of our

"Facility Personnel with Security Duties?" For instance, does a network administrator who may never physically set foot in a secure area now require a TWIC?

   b. Many facilities contract out some, or all, IT/OT functions, much like a contract for security officers to maintain access control. Would those contractors be required to maintain TWICs and be subject to 33 CFR 105.210 and 215? Some facilities utilize contracted security personnel as their FSO, which may be impacted without clear delineation of the FSO's qualifications and responsibility. Since cyber is now becoming more engrained and intertwined with the physical security aspects of regulations and guidance, some facilities may not be able to use contracted security FSO as an option, thereby increasing their overhead.
   c. Or, what if your IT data is stored offsite at a data center, is that facility required to meet these requirements?

4. *(p. 3.) Response to Change in MARSEC Level:* There should be a separate MARSEC Level for cybersecurity from physical security. The recommendation is to follow the ISO Standards and the NIST Standards. If we can increase MARSEC Levels based on cyber threats at an earlier stage, we could prevent a larger scale cyber and/or physical attack on our ports and on the nation. If we follow the current physical MARSEC Level protocol, we are too late.
   a. Transportation Security Incident (TSI) – We should not wait for a cyber incident to be a TSI to be a reportable cyber incident. If we are proactive and report immediately, the NCIC and NRS can begin to paint that common operating picture to determine if this is leading up to a TSI. I realize this is a lot to ask of a port with limited staffing, but it only makes sense. We should have customizable forms to report the incidents. I realize people will think this is too cumbersome, and do not have the staff to take care of it. However, it is essential to stay ahead of a potential nationwide impact, and there are tools that can be put in place to make reporting quick and easy.
   b. When we change MARSEC Level, what is USCG responsibility?
   c. What can we expect from USCG from a cyber perspective?
5. *(p.3.) Communications:* Facility operators should be able to communicate security conditions to and between the vessels, facilities and the Port Authority Chief of Police or Homeland Security Director, to the Captain of the Port, and to national and local authorities. Most ports are landlord ports, and it is important from an overarching port perspective for Port Authorities to be given access to security conditions at all their tenant facilities, in order to coordinate throughout the port. In physical security, if a facility has a physical issue such as a theft, they would contact their Harbor Police Department. Why wouldn't they contact them for a cyber incident? For example: Company ABC has vessels that are hacked and close down the channel to a port. The only entry to and from the port, this not only impacts that Company, but all facilities both MTSA regulated and all others as well as the Port Authority itself.

ENCLOSURE 2

1. *(p. 1.) Figure 1:* The smallest font on the graphic is a little hard to read.
2. *(p. 4.) IT/OT:* This is not defined in its first usage.

3. *(p. 8.) Section 3.1 and Table 1:* There is some confusion between the explanations of consequences in Section 3.1 and Table 1. Table 1 states that a catastrophic event would have physical consequences and makes it seem as if this is a requirement for an incident to be considered catastrophic. The definition in Section 3.1 mentions no physical consequences. Many times, a cyber event should be considered catastrophic due to impacts on commerce and will not include physical injury. The impacts of cybersecurity incidents on commerce need to be detailed further for easier differentiation between consequences and weighed heavier in determining the severity of a consequence. Overall, the two sources of definitions need to be uniform to prevent confusion.
4. *(p. 9.) Section: 3.2/3.3:* Encourage reference to use the CSET tool by DHS. It is far more comprehensive than the checklist provided in the appendix of the document. https://cset.inl.gov/SitePages/Home.aspx
5. *(p. 9.) Section: 3.2/3.3:* Will the NIST Framework that is laid out in Enc. 2 work for smaller facilities as the USCG presents it? Recommend Enclosure 2 be scaled to meet a small or large facility and division of responsibilities outlined can be tailored to meet the individual facility's needs.
6. *(p. 10) Section 4 of Enc. 2:* This is extremely important. I know it is difficult in this section, but I need to invoke the "Say what?" rule when I see "hash/checksums" and "Registration Authority." Aside from the occasional occult term, this section is pure gold. This section is like some of the classic NVIC job aids—the flowchart in 11-02 ch. 1, the checklists in 03-03 ch. 2, the detailed bulleted lists and extensive discussion in this section gives us strategies to reduce cyber risk.
7. *(p. 11.):* Physical is misspelled.
8. *(p. 13.):* Graphic is too small.
9. *(p. 16.):* OS is not defined in its first usage.
10. *(p. 17.) CG-5P Policy Letter No. 08-16:* The NVIC states to report security incidents based on current guidance and regulation. A reference to the current policy would be helpful, and contact information of who to report to should be provided. It is understood that by defining what breaches require reporting, limitations are placed that could prevent the communication of an event where disclosure is warranted. However, some guidance is needed to prevent the unnecessary reporting of innocuous incidents.
11. *(p. 21.) Recovery:* Recovery from a cyberattack is many times a complex process. Further guidance in this area would be helpful. Reference to NIST 800-184, which provides an in-depth guide to cybersecurity event recovery, is recommended.

RECOMMENDED ATTACHMENTS

1. *COMMON CYBER LANGUAGE:* Would like to see included as an attachment, the link to the Common Cybersecurity Language document created by TSSCWG the https://ics-cert.us-cert.gov/sites/default/files/documents/Common%20Cyber%20Language_S508C.pdf. This will assist the CRMT Facility Security Officers and the Chief Information Officers to have the common cyber language required to complete a Facility Assessment and Facility Security Plan. (Attachment A)

2. *CYBERSECURITY FUNDAMENTALS AND RESOURCES:* Would like to see an attachment with Cybersecurity Fundamentals and Resources for reference. This will aid everyone in ensuring we are cybersecure and provide the background for our FSOs and security folks who are just starting to become aware that cyber is part of their responsibility. (Attachment B)
3. *COMPUTER INCIDENT REPORT OR INCIDENT RESPONSE FORM:* Template for Reporting TSIs. Would like to see an attachment to help FSOs to work with their IT/OT Departments to gather information. (Attachment C)

AAPA 9/7/2017