American
Fuel & Petrochemical
Manufacturers

1667 K Street, NW
Suite 700
Washington, DC
20006

202.457.0480 office
202.457.0486 fax
afpm.org

October 11, 2017

Jason S. Warren
Office of Port and Facility Compliance
U.S. Coast Guard
2703 Martin Luther King Jr. Ave., SE
Washington, DC 20593

Attention: Docket ID Number USCG-2016-1084
Submitted to the Federal eRulemaking Portal (www.regulations.gov)

Re: U.S. Coast Guard's Request for Comment, "Navigation and Vessel Inspection Circular (NVIC) 05-17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities"

Dear Mr. Warren:

The American Fuel & Petrochemical Manufacturers ("AFPM") appreciates this opportunity to provide comments on the U.S. Coast Guard's ("USCG") "Navigation and Vessel Inspection Circular ("NVIC") 05-17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act ("MTSA") Regulated Facilities."[1] On July 12, 2017, USCG issued this draft NVIC, which proposes to clarify the existing requirements under MTSA to incorporate analysis of computer and cyber risks and guidance for addressing those risks. Many AFPM members' facilities are regulated under MTSA and will be impacted by the guidelines in the proposed NVIC.

I. AFPM's Interest in the NVIC

AFPM is a national trade association representing nearly 400 companies that encompass virtually all U.S. refining and petrochemical manufacturing capacity. Our members serve the American people by manufacturing virtually all U.S petroleum fuels and petrochemicals, strengthening economic and national security, and providing jobs directly and indirectly for over four million people. AFPM members have been at the forefront of cybersecurity efforts, participating in a wide-range of industry and government initiatives to enhance cybersecurity for critical infrastructure within the oil and natural gas ("ONG") and chemical sectors. Such efforts have included, but are not limited to, participation in:

- The National Institute of Standards ("NIST") Cybersecurity Framework Project ("NIST Framework" or "Framework");
- Department of Energy ("DOE") efforts to create a Cybersecurity Capability Maturity Model ("C2M2") for the ONG sector; and
- The Department of Homeland Security ("DHS") Critical Infrastructure Cyber Community ("C^3") voluntary program.

[1] 82 Fed. Reg. 32189 (July 12, 2017), https://www.federalregister.gov/documents/2017/07/12/2017-14616/navigation-and-vessel-inspection-circular-nvic-05-17-guidelines-for-addressing-cyber-risks-at.

Many AFPM member facilities are regulated under MTSA and have a vested interest in USCG cybersecurity efforts. Recently, AFPM assisted USCG in developing its 2016 Maritime Bulk Liquids Transfer Cybersecurity Framework Profile, as well as in establishing a streamlined protocol for reporting cyber-related incidents that could become Transportation Security Incidents ("TSI") at MTSA sites. In addition, AFPM has worked cooperatively with USCG in developing NVICs and Policy Advisory Circulars ("PACs") on various MTSA-related issues involving escorting, Transportation Worker Identification Credentials ("TWIC"), and MTSA compliance. Finally, many AFPM members belong to regional Maritime Security Councils, which work alongside USCG on national and regional security initiatives and information sharing efforts.

Given AFPM's collaborative relationship with USCG and our clear commitment to cybersecurity, we welcome this opportunity to provide comment on the cybersecurity guidelines laid out in the proposed NVIC.

II. Overview of the NVIC

MTSA facilities rely on computer-based systems to operate effectively. Historically, Facility Security Officers' ("FSO") responsibilities centered on physical security. While physical security remains critical to the operation of a site, MTSA facility security efforts must now address cybersecurity as well. This includes global positioning systems ("GPS") for vessels, industrial control systems, information technology, communications systems, alarm management and cargo screening technologies, and other components of a site that are dependent on computer-based tools. A cyber incident in any of these areas could affect the operation of a facility and potentially cause a TSI.

The NVIC reflects the USCG's concerns with possible cyber incidents at MTSA facilities and emphasizes the importance of implementing a cyber risk program at these facilities. The MTSA regulations in the Code of Federal Regulations ("CFR") (33 CFR Parts 105 and 106[2]) require MTSA-regulated facilities to analyze vulnerabilities in Facility Security Assessments ("FSA"). Enclosure 1 of the NVIC "provides draft interpretive guidance regarding existing regulatory requirements in 33 CFR Parts 105 and 106" and Enclosure 2 of the NVIC "provides draft guidance on implementing a cyber risk management governance program" based on the NIST Framework.[3]

The primary purpose of the NVIC is to clarify how existing requirements relate to cybersecurity measures and to provide recommendations on how a site's Facility Security Plan ("FSP") can be amended to address cybersecurity. Its secondary purpose is to provide MTSA sites with risk assessment tools for the development and implementation of cyber risk management programs.

---

[2] *See* https://www.gpo.gov/fdsys/granule/CFR-2010-title33-vol1/CFR-2010-title33-vol1-part105/content-detail.html and https://www.gpo.gov/fdsys/granule/CFR-2010-title33-vol1/CFR-2010-title33-vol1-part106.

[3] *See* http://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/DRAFT%20Cyber%20NVIC%2005-17.pdf?ver=2017-07-19-070240-737.

III. AFPM Supports the NVIC's Emphasis on the NIST Cybersecurity Framework

This NVIC provides guidance on how facilities can successfully implement a cyber risk management program based upon the NIST Framework[4] and other NIST documents. AFPM supports USCG recognizing the importance of a cyber risk management program for MTSA sites. AFPM agrees with this approach and strongly encourages USCG to continue to recognize its value in future NVICs and PACs.

In particular, AFPM is encouraged that the NVIC emphasizes the use of the NIST Framework. AFPM assisted in the development of the original Framework, released in 2014. Since then, AFPM has continued working with NIST on subsequent updates to the Framework and has assisted USCG in applying the Framework to projects such as the Maritime Bulk Liquids Transfer Cybersecurity Framework Profile. Finally, AFPM members utilize the NIST Framework as a tool in their own facility cybersecurity risk assessments, using it as guidance to better measure their facilities' cybersecurity risk management programs.

IV. Many of the NVIC's Guidelines Exceed USCG's Regulatory Authority Under MTSA

Under MTSA regulations (specifically, 33 CFR Parts 105 and 106), USCG is granted the authority to require that facilities' FSAs describe risks and vulnerabilities associated with the sites' "radio and telecommunication systems, including computer systems and networks."[5] This is the only language in existing MTSA statutes pertaining to cybersecurity requirements in FSAs.

However, the guidance outlined in the NVIC exceeds USCG's authority in prescribing what a facility must include in their FSA beyond requirements surrounding "radio and telecommunication systems, including computer systems and networks." For example, Enclosure 1 of the NVIC lays out additional general guidance for identifying cyber risks, including: cyber and physical security personnel coordination on developing cyber risk management programs, personnel training on cybersecurity matters, and drills and exercises to "test cybersecurity aspects of the FSP."[6]

The scope of the NVIC's guidelines exceeds USCG's regulatory authority, and any additional cyber-related requirements must be implemented only through formal notice-and-comment rulemaking.

V. The NVIC May Lead to Regulatory Uncertainty

While AFPM is encouraged that the NVIC emphasizes the use of the NIST Framework, AFPM notes that the lack of uniformity between the NVIC and the NIST Framework may lead to regulatory confusion.

Although there are other notable cyber risk management tools currently utilized by MTSA sites based on each site's individual needs (*e.g.*, C2M2 and C^3), the NVIC references only the

[4] *See* https://www.nist.gov/cyberframework.
[5] *See* https://www.gpo.gov/fdsys/pkg/CFR-2010-title33-vol1/xml/CFR-2010-title33-vol1-part105.xml.
[6] *See* http://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/DRAFT%20Cyber%20NVIC%2005-17.pdf?ver=2017-07-19-070240-737.

NIST Framework "as the recommended foundation for development of a cyber risk management program."[7] However, the guidelines set forth in the NVIC deviate from those of the NIST Framework: on the one hand, several of the NVIC's guidelines go beyond the recommendations put forth by the NIST Framework, and on the other hand, the NVIC does not incorporate the NIST Framework in its entirety. Ultimately, it appears USCG developed this NVIC by picking and choosing only certain portions of the NIST Framework and then exceeding this Framework by recommending additional steps for MTSA sites to take in developing a cyber risk management program. In doing so, the NVIC would serve as yet another set of industry guidelines on cybersecurity, potentially leading to regulatory uncertainty and inconsistent enforcement at MTSA sites and in turn causing these sites to expend unnecessary time and resources on identifying an appropriate cyber risk management program from the mix.

If USCG chooses to publish yet another set of cybersecurity guidelines for industry, we recommend that the NVIC: 1) identify the ways in which this set of guidelines deviates from and/or expands upon existing, widely-used cyber risk management tools (*i.e.*, the NIST Framework); and 2) explain USCG's reasoning behind these deviations. Doing so would alleviate potential uncertainty at the facility level, and enable industry to direct their efforts towards implementing the strongest possible cyber risk management program.

VI. NVIC and All Cybersecurity Guidance Should Remain Voluntary and Flexible

Each MTSA site is unique in its purpose, equipment, materials stored on site, personnel, site configuration, and security risks. For this reason, performance standards are preferable to a one-size-fits all command and control approach to security. We believe the Framework and other cybersecurity risk tools are, and will continue to be, most effective for critical infrastructure cybersecurity as a voluntary measure, as they provide a broad menu of options for businesses to fit their sites' differing and evolving needs. However, some of the measures referenced risk management tools that are not appropriate at all facilities. No two MTSA sites are alike; the needs of a site producing more than 325,000 barrels of crude per day differ from those of a site producing 26,000 barrels of crude per day. In addition, some sites use tankers and barges for transport, while others use trains, trucks, or pipelines. As such, there will be key variations in which tools MTSA facilities need in order to develop the best possible cyber risk management programs. Mandating a cyber risk management tool would not benefit MTSA facilities, as it would force these sites to adhere to cyber regulations that are harmfully rigid and not tailored to each individual site.

Moreover, cybersecurity threats are dynamic. Cyberthreats have evolved tremendously in the past decade and will continue to evolve in complexity. Consequently, there is virtually no way to accurately predict the cyberthreats of the future or the best way to address these vulnerabilities.

In comments submitted by AFPM to NIST on the original framework and on subsequent revisions, AFPM emphasized that the Framework should not be mandated through strict regulation.[8] That recommendation remains valid; the NIST Framework and any cyber-related

[7] *See* http://mtsanews.blogspot.com/2017/07/draft-navigation-and-vessel-inspection.html.
[8] AFPM Comments to NIST, April 17, 2017; "RE: Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity"

regulations should not become prescriptive, but rather remain voluntary guidance. This will allow greater flexibility in how industry responds to the dynamic nature of threats within the cyber arena.

VII. USCG's Expectations of How it Will Apply the NVIC are Unclear and Need to be Clarified

USCG does not indicate how it intends to apply the NVIC's guidelines. For example, it is not clear whether USCG expects facilities to submit new FSA Reports or amend existing FSA Reports in light of the NVIC**.** USCG must clarify how it expects to implement the NVIC in order to avoid regulatory confusion and facilitate compliance by regulated entities.

Furthermore, AFPM is concerned about the qualifications of USCG inspectors in relation to evaluating facilities' cyber risk management programs. It is important that any inspections done at MTSA sites be conducted by trained personnel, either from the USCG or a third-party contractor, who are familiar with this NVIC and the application of cyber risk tools at varied locations.

VIII. USCG Should Develop Guidance on Cyber TSI Boundaries and Connections for MTSA Sites

In a recent blog post, USCG noted that the purpose of the NVIC is "to assist the owner/operator in identifying cyber systems that are related to MTSA regulatory functions, or whose failure or exploitation could cause or contribute to a Transportation Security Incident [TSI]."[9] AFPM recognizes that TSIs are of grave concern to USCG and industry; however, it is important that USCG understand and clarify that not all cyber incidents at a site could cause a TSI.

AFPM therefore recommends that USCG develop clear guidelines on cyber TSI boundaries and connections for MTSA sites. Doing so would bolster USCG's efforts in encouraging the use of cybersecurity structure tools (*e.g.*, the NIST Cybersecurity Framework) and clarify regulatory compliance expectations for industry stakeholders and USCG inspectors.

IX. The NVIC is Limited in Scope

MTSA covers both facilities and vessels; however, the NVIC is limited to facilities and does not address vessels. To ensure the effectiveness of the cyber risk management tools implemented pursuant to NVIC, USCG should provide guidance that applies to vessels and offshore assets. A cybersecurity breach at a vessel or offshore asset could threaten the physical security of the facility, company personnel, and the general public and should therefore be equally protected. Each must have robust cyber risk management programs. This will ensure that all entities that fall under MTSA have equivalent and effective cybersecurity programs, preventing a weak link in the chain.

X. Conclusion

AFPM thanks USCG for the opportunity to provide input on this draft cybersecurity NVIC. AFPM recognizes that cybersecurity is a dynamic threat that could have direct consequences on

[9] *See* "Draft Navigation and Vessel Inspection Circular No. 05-17, Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Facilities," July 12, 2017, http://mtsanews.blogspot.com/2017/07/

MTSA sites. While we understand and appreciate the intent of the NVIC, we urge USCG to maintain the flexibility of cybersecurity risk management tools and guidance, address how USCG intends to implement the NVIC and ensure that inspectors are properly trained, develop guidance on cyber TSI boundaries and connections for MTSA sites, and address cybersecurity tools for vessels and offshore assets. These steps will enable more successful and efficient cybersecurity and compliance efforts.

AFPM looks forward to continuing to work with USCG on developing guidance on maritime cybersecurity standards. If you have any questions or if AFPM can be of any assistance in this process, please contact me at (202) 552-8475 or dstrachan@afpm.org.

Sincerely,

Daniel J. Strachan
Director, Industrial Relations and Program