NAWE

National Association of Waterfront Employers

8400 – WESTPARK DR • SECOND FLOOR • MCLEAN, VA 22102
202 587-4800 • www.nawe.us

October 24, 2017

The Honorable Michael McCaul
Chairman
Committee on Homeland Security
U.S. House of Representatives
2001 Rayburn House Office Building
Washington, DC 20002

The Honorable Bennie Thompson
Ranking Minority Member
Committee on Homeland Security
U.S. House of Representatives
2466 Rayburn House Office Building
Washington, DC 20002

Dear Chairman and Ranking Member

I am writing on behalf of the National Association of Waterfront Employers (NAWE) to provide comments pertinent to the House Committee on Homeland Security's field hearing on "Examining Physical Security and Cyber Security at our Nation's Ports." NAWE is the voice of marine terminal operators (MTO) and stevedores and has participated in discussions of these issues since the enactment of the Maritime Transportation and Security Act of 2002 and its implementation by the United States Coast Guard (CG). Marine terminal operators buy and operate equipment and hire labor to act as the master link in the global intermodal marine transportation system. The oft characterized importance of the economic contribution by this system cannot be underestimated.

The Department of Homeland Security (DHS) under the Authority of the Congress and the leadership of successive Presidents has orchestrated a system of layered physical security in addressing threats made apparent following 9/11. This layered security includes international port assessments and container inspections by the CG and United States Customs and Border Protection (CBP). It includes advanced notices of arrival and offshore boarding by the CG and CBP. And it includes compliance with CG and CBP regulations by marine terminal operators who form the membership of NAWE. Specifically, it is the marine terminal operator who must have an approved Facility Security Plan (FSP), a designated Facility Security Officer (FSO) and obtain releases for cargo from CBP's Automated Customs Environment (ACE). Recently, NAWE was deeply involved in the planning for a Transportation Workers Identification Card biometric reader and response to the CG's request for comments to its draft Navigation and Vessel Inspection Circular. It is also the MTO that is singularly focused on the success of the business, attending to the diverse objectives of productivity and safety/security. Today's safety/security preserves tomorrow's productivity. NAWE and its members are committed to ensuring that our port's physical and cyber security remain the best in the world.

Physical Security.

Following 9/11, NAWE and it members partnered in the formulation the layered physical security for the global maritime supply chain through the various public forum including local Area Maritime Security Committees. NAWE's members are today a significant investor in and

integral component of this system. Efforts in foreign ports and on the high seas/customs waters go relatively unnoticed. However, the continued efforts of the marine terminal operator to be most productive in transferring cargo as the master link in our nation's cargo chain receive continuous review as necessary to meet their responsibilities under MTSA, the FSP, and the goals of layered security for our ports. The marine terminal operator must evolve and improve while CG and CBP regulations remain constant. The question is whether CG and CBP regulations are able to blend the need for strong security and commercial efficiency.

NAWE applauds the CG's and other agencies current efforts to review its security regulations. However, NAWE seeks continued cooperation with the CG and CBP to develop a unified DHS port security approach including developing a "one-DHS" approach to the FSP and Customer Trade Partnership (CTPAT) as indicators of our collective commitment to the nation's maritime security. With this much needed review of regulations and the potential for Congress to act to reauthorize DHS, we see an opportunity to not only improve security at our nation's ports, but to also improve on the public private partnerships that are key to that security. NAWE hopes these actions can result in improved security that works seamlessly with much needed advancements in commercial efficiencies. If changes to laws and regulations governing our nation's physical port security are made with input from private sector partners, NAWE believes both goals can be achieved.

Cyber Security.

One need only review the morning news to understand the critical role of strong cybersecurity in our nation's ports. To understand NAWE commitment to cybersecurity, I refer the Committee to NAWE's published response to the CG NVIC 05-17. The NVIC describes the CG interpretation of MTSA to include Cyber requirements throughout the FSP as well as forecasting a "governance" process for the future. Two underlying principles are contained in this response: (1) While MTSA provides clear authority over physical security in protection against kinetic threats, it does not do so over the broad cyber spectrum and (2) NAWE and its members strongly endorse vigorous and vigilant attention to cyber security.

First, a few comments on the nature of cyber and cyber systems at port operating facilities. Cyber as something of value is not likely to be the servers and various data terminals, it is likely to be the "information" or "data." Further, the real value is not solely in the information or data, it is in the capability to distribute the information or data within and beyond the facility. It is this distribution capability, especially beyond the facility, which also becomes its vulnerability. This capability is called the World Wide Web – it's the global cyber space.

At port operating facilities you will find the HR, finance, and scheduling capabilities existing at every business of similar size and sophistication around the country. Unique cargo moving systems include load planning, terminal operating systems (TOS), and customs' release authority. Load planning if not on a white board is often done at a centralized location and customs' release is done by the government. The piece of cyber most key to port operations are

the TOS. Various terminal operators do not use the same system or even a consistent level of capability. Some operators might be able to function adequately without a technology solution, some could no longer. Higher end TOS often represents proprietary software and included security measures from the start.

Regarding the record of cyber "incidents," there have been several examples: releasing cargo (contraband) to the wrong recipient at a European facility, ship to shore cranes losing GPS feed, and recently malware which shut down operations at a global operating company. What were the impacts, the causes, the vulnerabilities, and the threats? Was data or cargo compromised? Did they impact the nation's marine transportation system or even the port-wide system? Are there unifying recovery actions available? What actions, if taken by the Congress or DHS, would have prevented them? These are important questions. MTSA sets out a requirement for assessments such as these questions prior to formulating responsive plans.

As a unifying theme connecting NAWE's first two observations and the following cyber basics, significant public private partnerships occurred in the development of MTSA physical security in protection from kinetic events. Out of that partnership came the articulation of a "transportation security incident (TSI)." No such discourse or set of definitions exist today with respect to cyber. In fact, NAWE members observe disparate characterizations by the CG of last summer's port cyber security event impacting several US port operations. Some have not even recognized that the "event" occurred outside the US. At a minimum, the nation and DHS is not prepared to establish policy to provide security from cyber intrusions. Although not able to substantiate its assertion, NAWE believes its members (particularly those most dependent on cargo cyber systems) have as good of understanding of and response to cyber security imperatives as the DHS components. NAWE's members are certainly incentivized. This raises the question of whether there is a value-add in governmental well-intended efforts or whether the market place is the better incentivizing arena for the port operator's sector. As we develop further technology solutions NAWE members continue to spur better cyber security.

NAWE observes recent discussions of the importance of "personal" actions in vulnerabilities and protective measures in cyber security. It is interesting that "people" have been raised as more important than technology to cyber security at the same time that the full anticipated value of TWIC biometric readers to physical security at marine terminal operations has been reduced.

NAWE's members acknowledge the existence of the NIST framework for cyber security. It has value, but is its value in having a lockstep citation within a facility security plan as presented in the recent NVIC or is it a means for the growing cyber security industry to be guaranteed work. NAWE members and their cyber security teams go beyond frameworks and look for the best practices to assure protection of their data and business practices from unwanted intrusions. Are best practices an effort that the Congress and DHS can contribute to and how? Is it one that even the disparate terminal operators can gain from working together? These are important questions, yet hard to answer. NAWE is available to continue this discussion.

NAWE members value the CG's protection of SSI information and CBP's efforts to maintain ACE in the face of cyber-attacks. Members also value nationally accessed information not commercially available which might stimulate the most valuable cyber security measures. Like the physical security realm, NAWE members would value national efforts to defeat global criminal and terrorist networks which are the source of many attacks. These efforts might extend to foreign shores but at least should preserve the use of the global cyber space (also known as the World Wide Web) for peaceful and economic purposes as is done for commerce on the high seas. Following events, NAWE members recognize the value of the CG, CBP and Port Authorities in recovery efforts. These are the kind of efforts DHS (specifically the CG) addressed contemporaneously in developing MTSA and FSP requirements.

NAWE asks that Congress support these efforts of DHS mission focus and most important to the safety and security of our nation's ports, support the direct involvement of the marine terminal operators in the development, implementation, and execution of port security policies. For NAWE and its members to be effective partners, they need to know that the agencies we work with are empowered to be partners at every step. NAWE members are committed to their contributions to the global marine transportation system, the stimulation of the best productivity possible and the preservation of businesses, jobs, and lives through state of the art safety and security practices.

Sincerely,

John Crowley, President
National Association of Waterfront Employers (NAWE)