AAPA American Association of Port Authorities

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

Seaports Deliver Prosperity

December 12, 2013

Information Technology Laboratory
Attention: Mr. Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Dear Mr. Sedgewick:

The American Association of Port Authorities' U.S. members appreciate the opportunity to comment on the preliminary version of the voluntary Critical Infrastructure (CI) Cybersecurity Framework prepared by the National Institute of Standards and Technology (NIST) to assist constituents of designated CI sectors with improving cybersecurity standards.

AAPA members represent deep-draft public port agencies throughout the United States, including on the West Coast, East Coast, Great Lakes and Gulf of Mexico. These port authorities are arms of state, local or regional governments and are responsible for handling more than 99 percent of the nation's overseas trade, in addition to processing millions of cruise passengers each year and serving as a front line on homeland security and stewards of critical coastal natural resources.

Member port authorities range from large to small and handle a wide variety of cargos, including containerized cargo, bulk and break bulk commodities and roll-on/roll-off cargo. Some ports are hubs for reaching consumers, manufacturers and agricultural exporters in the interior of the country; others play a vital and irreplaceable role for their community or a niche industry.

The Framework, the implementation of which should remain voluntary, is an important component in the relationship that ports have with the federal government in creating greater cybersecurity as laid out in the Executive Order dated February 12, 2013, while also maintaining the independence and flexibility necessary to appropriately implement standards within their respective organizational structures. The Framework represents a minimum level of cybersecurity attention, meaning that it may not provide sufficient guidance to all relevant parties who choose to implement its provisions and suggestions.

AAPA and its member port authorities find a great deal of value in the Framework's stated goal of establishing a common language for use in discussing cybersecurity. As this issue continues to emerge, evolving rapidly all the while, there is a need for clarity in communication about goals, strategies, objectives and tactics. To ensure that the federal government, state and local partners and security experts are communicating clearly and efficiently, common language will be critical.

1010 Duke Street, Alexandria, VA 22314-3589 p 703.684.5700 f 703.684.6321 www.aapa-ports.org

Building on existing success is also important. To that end, AAPA is supportive of efforts to utilize and reference existing standards, including those from NIST and the International Standards Organization. Taking advantage of existing standards ensures that efforts within the federal government will not be duplicated, and it increases the chance of compliance as organizations can be assured that the Framework builds on best practices and requirements and does not compete with them.

While AAPA finds value in making distinctions between the various tiers of implementation, the Framework does not make it easy or intuitive for the user to determine where his/her organization falls within the tiers or to which tier his/her organization should aspire. A voluntary self-assessment tool within each tier would make that portion of the Framework more meaningful to a user.

Similarly, the Framework would be more useful were it structured in a way that better addresses the differences within CI agencies, by allowing more flexibility for organizations to implement the Framework. Explicitly addressing compensating controls, for example, would allow CI agencies of different sizes and structures to achieve some form of implementation that makes sense for their organizations. The Framework should discuss the use of compensating controls in its current form, rather than in a later iteration, in the context of a risk assessment that an organization uses to identify its goals and the risk it is willing to assume.

A greater emphasis should be placed on Industrial Control Systems, such as for Supervisory Control and Data Acquisition (SCADA). SCADA systems have not necessarily been designed to be secure from an Information Technology perspective, and therefore there must be more discussion about limiting physical access to core facility systems.

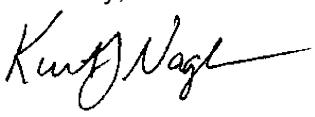
Like other public agencies defined as CI, port authorities have on-going relationships with federal agencies in creating physically secure environments. Generally the Framework may be more beneficial in some respects were a larger discussion made about working with federal agencies in defining the necessary scope of protection. While there is mention of working with local law enforcement, for example, the potential is not sufficiently discussed for partnering with agencies such as the U.S. Coast Guard (USCG), which is the lead agency for port security, while both we and USCG work to learn more about port cybersecurity needs. Ports, as well as other agencies and sectors of CI, have worked to implement physical security standards, hardening a key portion of the nation's border infrastructure against terrorism and crime. As the federal government works to ensure the cyber assets of these entities are similarly hardened, the Framework would be more relevant to port authorities if it discussed how physical security goals and objectives can and should align with cybersecurity goals and objectives.

Finally, AAPA believes that the Framework, unfortunately, falls short of its goal of giving business leaders an understanding of complex cybersecurity implications. The Framework does not communicate at an appropriate level for business leaders; it is more technical in nature and geared toward information technology officers. More helpful to port executives would be a discussion of the strategic importance of

cybersecurity including more discussion of the framework's objectives, and a high-level overview of the core functions, including how those functions relate to other business goals. We recommend that the Framework direct the use of the tiers as the method of communicating cyber readiness to executives and boards. In that regard, the tier definitions will need further refinement, but their usage is preferable to using the technical details of the profile.

Again, we appreciate the opportunity to comment on the NIST Framework. Please feel free to contact me if you have any questions.

Sincerely,



Kurt J. Nagle
President and CEO
KJN:kp/lsm