AAPA American Association of Port Authorities

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

Government Relations Priorities

Cybersecurity

Increased awareness of cyber vulnerabilities at ports is necessary not only for Information technology and security professionals but also for maritime leaders and our partners in Congress and executive agencies. The growing reliance on automated systems makes the domestic and global supply chains vulnerable to potential criminal and terrorist cyber attacks. The flow of goods through ports is dependent in large part on networked computer systems, controlled by human operators, but that also work independently and are programmed to move containers and goods in a very precise, orchestrated manner. Should these processes be compromised, a cascading effect might be created, disrupting the goods movement supply chain through ports and across the entire country.

Port information technology leaders, along with their counterparts in private industry and other critical infrastructure (CI), have been confronting the threat of cybersecurity for some time. However, the issue of cybersecurity continues to grow in prominence and gain attention, evolving rapidly, and 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 is critical.

Several ports have participated in the General Accountability Office's cybersecurity review of ports, and others are working with local and federal law enforcement, as well as academic institutions, to identify and implement best practices on cybersecurity.

At the federal agency level, there is a need for common standards and a clear delineation of roles and responsibilities for CI, including ports.

For AAPA member ports, the top three priorities are implementing the Presidential order on cybersecurity, defining the U.S. Coast Guard's role and providing federal funds through the Port Security Grant Program (PSGP).

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) released their cybersecurity framework in February 2014. 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.

The Framework, the implementation of which should remain voluntary, will be 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 draft Framework represents a minimum level of cybersecurity attention.

Additional measures will be necessary to meet commercial "Standard of Care" cybersecurity levels and other standards such as the Payment Card Industry (PCI) standard, HIPPA, and Sarbanes-Oxley and other cybersecurity standards may also apply to a particular port as a result of their business practices. Many States also have legislative and regulatory requirements relating to protecting the personally identifying information of employees and customers which will need to be incorporated into the cybersecurity profile.

I. Tiers of Implementation and Risk-Based Implementation

While AAPA finds value in making distinctions between the various tiers of implementation, the Framework does not make it easy or intuitive for a 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.

Using a risk-based approach to defining an individual Port's cybersecurity requirements is highly recommended and requires input and acceptance from the Executive and Governing Board levels of a Port.

Using a formal risk-based assessment to determine acceptable and unacceptable risks at the Governing and Executive levels enables Ports to make informed decisions when determining investment levels and priorities.

II. Compensating Controls

Explicitly addressing compensating controls allows CI agencies of different sizes and structures to achieve some form of implementation that makes sense for their organizations. Compensating controls should be discussed in the context of a risk assessment that a particular organization currently uses to identify its goals and the risk it is willing to assume.

III. Relationship with Physical Security

Like physical security, which continually adapts to changes in buildings and new threat vectors, cybersecurity also requires an ongoing commitment to responding to the rapidly changing cyber threat environment.

Just as annual physical security exercises are conducted to ensure good working processes, annual cybersecurity exercises are recommended and should include a port's law enforcement partners to ensure appropriate notifications, forensics preservation, and investigation processes meet the port's needs.

Coast Guard's Role

Like other public agencies defined as CI, port authorities have on-going relationships with federal agencies in creating physically secure environments. Any efforts to establish best practices or create a framework for managing cybersecurity must include a clearly defined role for the U.S. Coast Guard (USCG), which is the lead agency for port security. Tasking the USCG with responsibilities for cybersecurity within ports is logical but will strain an agency that has already seen its mission and responsibilities expand greatly since 9/11. Any expansion of the USCG's role should be accompanied by additional resources to ensure that the agency can meet new demands without compromising any of the other vital duties they have with respect to ports and the maritime industry.

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 that the cyber assets of these entities are similarly hardened, federal policy at all levels 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.

Port Security Grant Program (PSGP)

It is important that the existing PSGP within the Department of Homeland Security continues to prioritize cybersecurity. Since implementation of the Maritime Transportation Security Act following 9/11, PSGP funds have been critical in raising the standard of physical security at ports throughout the United States. The value of the PSGP in addressing cybersecurity will continue to rise as ports seek to meet the challenges of this growing threat.

In California, ports are utilizing PSGP funding to stage a tabletop cybersecurity exercise in spring 2014, and the results of this exercise may provide further illustration and information about how to best utilize PSGP funds for cybersecurity purposes.

March 2015