AAPA American Association of Port Authorities

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

Government Relations Priorities

Maritime Security

Seaports are international borders and gateways to America, therefore, the federal government has a clear Constitutional responsibility to protect them. AAPA member port authorities have worked for many years in cooperation with federal agencies like the Department of Homeland Security (DHS) and others. It is imperative that this relationship between ports and their federal partners remains strong in order to continue protecting the United States from potential grave threats posed against our seaports and against our nation as a whole.

I. PORT SECURITY GRANTS

The Port Security Grant Program (PSGP) continues to be very valuable for U.S. ports, which serve as partners with the Department of Homeland Security (DHS) to harden security and protect our homeland.

Grant Funding Eligibility. In the FY 2017 House and Senate appropriations bills, PSGP was funded at $100 million. AAPA urges Congress to continue funding this program as a line item, and to increase the authorization and appropriation levels for the program back to where it once was at $400 million. Unfortunately, the President's FY 2018 budget proposed a 52 percent decrease for PSGP, down to $48 million. (The House FY 18 DHS appropriations bill includes $100 million and the Senate has not yet marked up their bill).

AAPA is concerned that drastic cuts in recent years to the Federal Emergency Management Agency's (FEMA) preparedness grant programs, including PSGP, threaten the ability of our nation to maintain or expand our current level of security.

PSGP has funded patrol vessels, video surveillance and access control systems, TWIC readers and infrastructure, sonar equipment, cybersecurity assessments, and numerous other projects to enhance maritime domain awareness and improve response and mitigation capabilities of first responders.

Finally, AAPA would like to see more of the PSGP funding go directly to port authorities. With emerging threats, such as cybersecurity, grants to port authorities need to be a priority.

II. FULLY FUND CBP AND STAFF MARITIME ACTIVITIES

Each year, roughly 1.2 billion metric tons of foreign trade cargo, including more than 11 million cargo containers, arrive at our seaports. Additionally, over 11 million international passengers begin their cruises via U.S. seaports. U.S. Customs and Border Protection (CBP) is on the front line when cargo and passengers enter our country. CBP officers meet the ships at all ports of entry to check the manifests, screen incoming cargo, operate nonintrusive inspection (NII) equipment including radiation portal monitors, provide specialists to examine imported fruits, vegetables and flowers for potentially harmful diseases, and other missions at our busy gateways. CBP is also responsible for screening all foreign visitors and returning American citizens and passenger ships that enter U.S. seaports.

In order for America's international gateways to function more efficiently, effectively and safely, CBP must be adequately funded and staffed. In FY 2015, when CBP was funded to hire 2,000 additional staff, fewer than 20 agents were assigned to seaports. This inequity of CBP resources cannot continue. Our nation's ports are in partnership with CBP in securing our supply chain and providing vital support in moving freight safely through our ports and out on to the national freight network.

CBP estimates that it is short 500 officers in the maritime environment. To address a shortage of staff and funds, Congress authorized a new Section 559 program that allows for reimbursable services and donation agreements. While this program can be helpful to enhance the efficient movement of maritime cargo, it is not a long-term solution. This program is not flexible for short-term needs, must compete for limited overtime hours for CBP officers and establishes an unfair playing field, where some ports have to pay for CBP services, while other ports do not have to pay. The cost can be substantial for these services.

We strongly urge Congress to increase CBP FY 2018 funding and staffing resources directed to maritime activities.

III. NUCLEAR DETECTION

Non-Intrusive Inspection (NII) Technology. Ports are in compliance with the 2002 and 2007 laws mandating that cargo scanning take place to prevent nuclear or other radiological devices from entering the United States.

Evidence collected by the DHS Office of Inspector General shows that CBP and the Domestic Nuclear Detection Office do not have a plan for continuing maintenance, replacement, or funding for these machines (e.g., Radiation Portal Monitors, VACIS, etc.). Ports should not be required to fund this security program, initiated by the federal government in order to secure international borders. Congress provided some funding in FY 2016, but sustained and predictable funding is needed.

AAPA requests that DHS conducts a study on how the agency intends to pay for the future use of scanning equipment, when such equipment must be modified and moved due to port facility expansion or reconfiguration, and for the replacement of current scanning equipment that has reached the end of its useful life.

100 Percent Scanning. AAPA encourages DHS to continue carefully evaluating the viability of implementing the 100 percent scanning mandate and to avoid instituting a system that will slow cargo movements or significantly increase the cost of shipping. AAPA is also concerned about reciprocity should other nations require 100 percent scanning of our exports.

IV. CYBERSECURITY

As the federal government seeks to increase its role in protecting critical infrastructure from cyberattacks, any models or frameworks must continue to be voluntary and industry led. It is important for USCG, the lead agency for port security, to be given the resources and training necessary to understand the individual security requirements of each port and facility so that the agency can provide effective support in the cybersecurity arena.

- AAPA supports the National Institute of Standards and Technology (NIST) which released its 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. Implementation should remain voluntary.
- AAPA recommends 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.
- AAPA recommends that just as annual physical security exercises are conducted to ensure good working processes, annual cybersecurity exercises are recommended and should include ports' law enforcement partners to ensure appropriate notifications, forensics preservation, and investigation processes meet ports' needs.

V. CRITICAL INFRASTRUCTURE RESILIENCY

Natural disasters, terrorist attacks, and other crises cause billions of dollars in damage to power, water and other key infrastructure, resulting in lost economic activity when they occur at seaports. Programs at DHS and other federal agencies can increase port resiliency against such events by bolstering information sharing and providing grants for projects to enhance resiliency. These programs can help ports to create effective disaster implementation plans and exercises for restoring normal operations.

VI. SUPPLY CHAIN SECURITY

While DHS has attempted to address supply chain security under various CBP programs, the reality is that no internationally agreed upon minimum supply chain security standards have been established. Without this global baseline, and a method of either enforcement or rewards, supply chain security is largely voluntary with little chance of truly enhancing security.

A framework for minimum mandatory supply chain security standards that is recognized and accepted worldwide is necessary to begin the complex process of ensuring that goods moving through the supply chain are not compromised.

VIII. RESEARCH AND DEVELOPMENT

DHS should devote more resources to maritime security and work closely with the industry on priorities. For example, DHS could work with ports on the protocols they use, and conduct R&D to encase and shield a suspect container that is being shipped to an inspection area. In all areas of R&D, DHS should work closely with port facilities to ensure that new systems and technologies can be efficiently integrated into port operations.

September 2017