ESSENTIAL. RESILIENT. UNITED.
SEAPORTS DELIVER

Government Relations Priorities

Port Security

Seaports serve our nation as international borders of protection and gateways to economic prosperity. Because of the critical, indispensable purpose's ports serve to the nation, it is thus the government's responsibility to protect the ports and the assets they provide.

PORT SECURITY GRANTS

The Port Security Grant Program (PSGP) continues to be a vital source of income for U.S. ports. The PSGP protects our country, our workers, and our supply chains. Ports large and small use these grants to stay vigilant, to 'harden' their facilities and networks, and to prepare for potential attacks. Our understanding about what threats look like are evolving and the PSGP is evolving, too.

U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) allocates the PSGP after the program is funded by Congressional appropriation. For Fiscal Year 2020, Congress provided $100 million to over 30 U.S. port authorities, along with numerous terminal operators, municipalities, and policing entities, to help protect critical port infrastructure from terrorism, enhance maritime domain awareness, improve port-wide maritime security risk management, and maintain or reestablish maritime security mitigation protocols that support port recovery and resiliency capabilities.

AAPA continues to advocate for increased PSGP funding to address port and maritime security needs. PSGP has funded patrol vessels, video surveillance, 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 believes more funding of the PSGP should be funneled directly to port authorities. Of the total funds allocated through this grant, only 26.277% was allocated to port authorities. As threats continue to emerge, directly targeting supply chains, allocating funds to protect our nation's economy needs to be a top priority.

FULLY FUND CBP AND STAFF MARITIME ACTIVITIES

Two of AAPA's highest advocacy priorities are CBP facility and staffing demands. Each year, roughly 2 billion metric tons of foreign trade cargo, including more than 23 million cargo containers, arrive at our seaports. Beyond cargo, 12.2 million international passengers begin their ventures via U.S. seaports. U.S. Customs and Border Protection (CBP) is on the front line when cargo and passengers enter our country, inspecting and vetting the products and people who come and go from our nation. Port authorities recognize and appreciate the important work CBP does and the critical role they play within the transportation industry.

However, we also recognize the multiple instances in which CBP has taken advantage of and attempted to extort port authorities out of facility space and resources, due to their own lack of funding. For America's international gateways to function more efficiently, effectively, and safely, **CBP must be adequately funded and staffed.** With proper funds being allocated to CBP, they will be able to better

perform their duties and carry out their agency's mission without being reliant upon ports to support their infrastructure and staffing needs.

CBP staffing shortages have recently reached numbers in the high hundreds. In order to curtail a small portion of these shortages, Congress authorized a Section 559 program that allows for reimbursable services and donation agreements, allowing ports the opportunity to donate space and services to CBP as they wish. This program is beneficial to the industry as a whole, encouraging cooperation and participation between parties. However, CBP has begun to weaponize the gratuitous intent of this program, making strong demands to ports with threats to operations if not conceded to. If CBP was properly funded and supported by federal funding, this problem would be sparse, if existent at all. We strongly urge Congress to increase CBP funding and staffing resources directed to maritime activities in order to alleviate pressure being felt by ports around the nation.

CYBERSECURITY

Due to the wealth of information it provides, critical infrastructure has become a high-value target for cyber-attacks. As threats to the maritime and transportation industry continue to evolve, so must the security protections against them. Maritime cybersecurity is a unique facet that must be recognized as such by not only port security teams, but the federal government. AAPA fully supports the initiative that the appropriate resources and training necessary be allocated to the U.S. Coast Guard to understand the individual security requirements of each port and facility. This will allow the agency to provide effective support in the maritime cybersecurity arena. AAPA backs the National Institute of Standards and Technology (NIST), which released its cybersecurity framework in February 2014.

AAPA recommends that the existing PSGP within the Department of Homeland Security continues to prioritize cybersecurity. The PSGP provides funding to secure and modify equipment, software, and other infrastructure that is critical to maintain the cyber health of ports and thus, trade. According to FEMA, the agency gave priority consideration for projects that enhance cyber security, enhance protection of soft targets/crowded places; enhance weapons of mass destruction and improvised explosive device prevention, detection, response and recovery capabilities; and address emergent threats, such as unmanned aerial systems. Funding should remain focused on these critical improvements.

Amid the Coronavirus pandemic, increased risk to OT systems have become apparent due to crossover with IT systems. This lack of seperation means that if compromised, a cyber-attack could directly affect port operations, and have the potential to cause significant cascading supply chain effects. There is a need to address the new attack surfaces associated with IT/OT convergence. This can be done by adopting a unified view across the entire infrastructure, which requires gaining deep situational awareness of each and every asset and vulnerability.

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. As we have seen most recently, cyberthreats are opportunistic. Therefore, ports must remain vigilant at all times so that in the event of an emergency, their systems are protected from attempted exploits. Dedicated and consistent monitoring alongside action plans are the key factors to reducing the possibility of a cyberattack.

CRITICAL INFRASTRUCTURE RESILIENCY

As seen throughout the novel Covid-19 pandemic of 2020, crisis can occur at any time, effecting each industry in a unique but devastating way. Loss of economic activity at seaports can occur through a variety of disasters, but none that have been felt as hard as during the coronavirus.

Essential preparation, following FEMA protocols and those of other government agencies, can alleviate the financial strife felt by ports during trade falls. 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. Disaster relief plans, lost revenue analysis, and emergency cost tracking can help ports to create effective emergency implementation plans and exercises for restoring normal operations.

SUPPLY CHAIN SECURITY

While DHS has attempted to address supply chain security under various CBP programs, such as C-TPAT, the U.S. Customs –Trade Partnership Against Terrorism, and CSI, the Container Security Initiative 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.

There is a strong need for minimum mandatory supply chain security standards that are recognized, accepted, practiced and most importantly, enforced, worldwide. Ensuring that goods are moving efficiently and responsibly through local, national, and global supply chains is essential to the protection of the trade industry.