STATE OF FREIGHT IV

SECURING AMERICA'S PORTS AND ENHANCING THE SUPPLY CHAIN

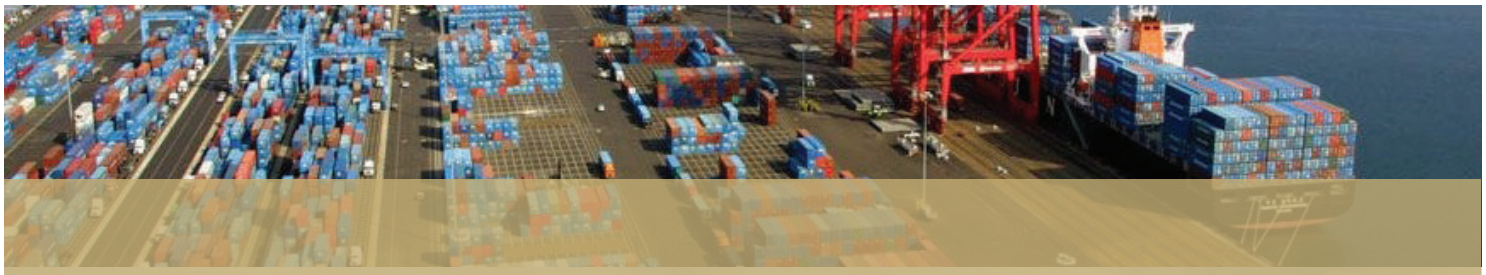
Looking Ahead at the Challenges and Opportunities Facing the Port Security Grant Program

PORT SECURITY GRANT PROGRAM REPORT

AAPA American Association of Port Authorities

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

DECEMBER 2018



In the 17 years since 9/11, freight and passenger volumes have increased significantly at U.S. ports. Between 2001 and 2017, container volumes increased by 71 percent, total foreign trade in short tons increased by 37 percent, and passenger traffic at U.S. cruise ports increased by 98 percent.

PORT SECURITY GRANT PROGRAM REPORT

December 2018

PORT SECURITY GRANT PROGRAM REPORT

EXECUTIVE SUMMARY

America's ports are a critical piece of our nation's goods movement network, ensuring that U.S. exports reach the global marketplace and that U.S. manufacturers and consumers have reliable, cost-efficient access to the products they rely on. In its "State of Freight" series, AAPA has highlighted the transportation infrastructure needs of U.S. ports, state transportation agencies and multimodal projects. In this final report in the State of Freight series, AAPA turns to the vital role that security infrastructure plays in moving goods.

In 2002, Congress created the Port Security Grant Program (PSGP) as part of the direct response to the tragic terrorist attacks of 9/11. According to the Federal Emergency Management Agency (FEMA), the PSGP has funded 8,096 projects and invested more than $2.78 billion in America's ports in the past 16 years. More than a decade and a half since the PSGP began, it remains a top priority for the American Association of Port Authorities (AAPA).

To better understand what future security challenges U.S. ports, their communities and supply chains face in the next decade, in 2018 AAPA surveyed its U.S. corporate members on how this program has impacted security at their ports and, ultimately, goods movement. AAPA members reported they will need $2.62 billion to maintain and at times upgrade their security apparatus over the next 10 years. AAPA members also identified $1.27 billion in future security investments to address cybersecurity, active shooter, drone mitigation, resiliency or other evolving security threats. In total, a sustained investment of $3.89 billion ($4 billion) will be needed between 2019-2028. Ninety-five percent of AAPA's U.S. corporate members responded directly to this survey and provided feedback in follow-up interviews.

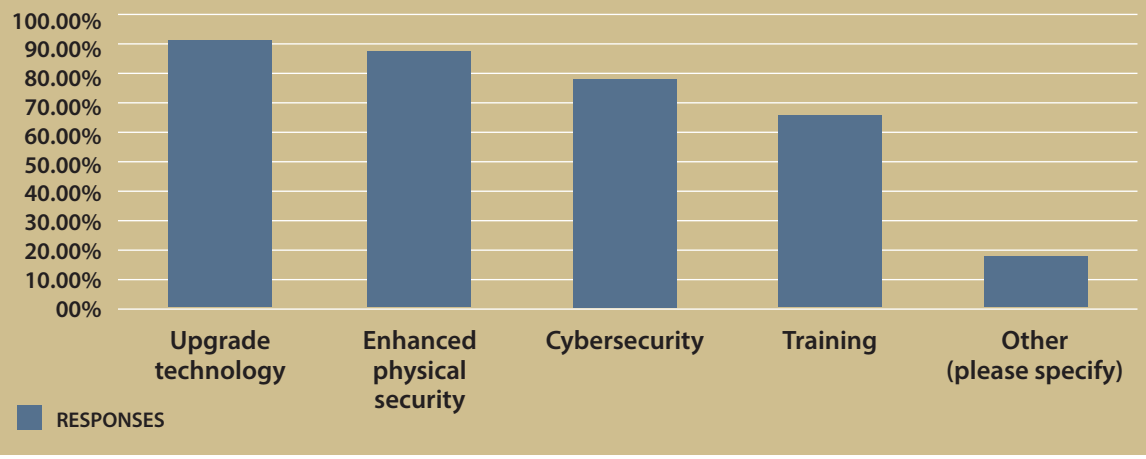
NEW THREATS, EVOLVING SECURITY APPROACHES

Since 9/11, the U.S. population has increased by 15 percent with a pronounced shift to metropolitan areas where residents live in densely populated urban areas, including near port authority facilities that support both freight and passenger activity. In the 17 years since 9/11, freight and passenger volumes have increased significantly at U.S. ports. Between 2001 and 2017, container volumes increased by 71 percent, total foreign trade in short tons increased by 37 percent, and passenger traffic at U.S. cruise ports increased by 98 percent. When asked if their ports' security costs increase proportionally to the growth in their ports' freight or cruise volumes, 55 percent of the ports reported "Yes." In earlier years of the programs' authorization, the PGSP had been funded at $400 million a year. Currently, the federal government invests just $100 million annually in the PSGP to protect one quarter of the nation's Gross Domestic Product that moves through America's ports.

> The State of Freight IV Port Security Grant Program Report finds that ports will continue to need a port security grant program that is administered efficiently as well as funded adequately to meet the current and emerging security risks.

What do you anticipate spending PSGP funding on over the next ten years?

(Check all that apply)



BASED ON THE SURVEY RESULTS AND FOLLOW-UP INPUT FROM U.S. CORPORATE MEMBERS, AAPA PROVIDES THE FOLLOWING RECOMMENDATIONS:

1. Fund the PSGP at a minimum of $400 million annually.

2. Keep the administration of the Port Security Grant Program in FEMA.

3. Designate within the Notice of Funding Opportunity that a minimum of 50 percent of the PSGP allocation be awarded to projects submitted by public port authorities and law enforcement and emergency response agencies directly responsible for the day-to-day safety and security of the port complex. Remaining funds would be allocated to projects submitted by designated Maritime Transportation Security Act (MTSA) regulated facilities and projects submitted by law enforcement and emergency response agencies responsible for secondary support of the safety and security of the port complex.

4. Focus the funding on the latest and emerging threats to our ports, communities and supply chains including cybersecurity, active shooter and drones.

5. Conduct in coordination with each COTP an updated port wide risk assessment inclusive of the latest threats and consider updating port wide strategic risk management plans to establish a new baseline.

6. Mandate that the local Grant Field Review Teams (GFRT) have equal representation of all stakeholder groups including local port authorities and representatives of the container, petrochemical, ferry, cruise or other impacted sectors as appropriate. Protocols should be established within each Area Maritime Security Committee (AMSC) so that a member of the GFRT cannot vote or comment on their own grant application.

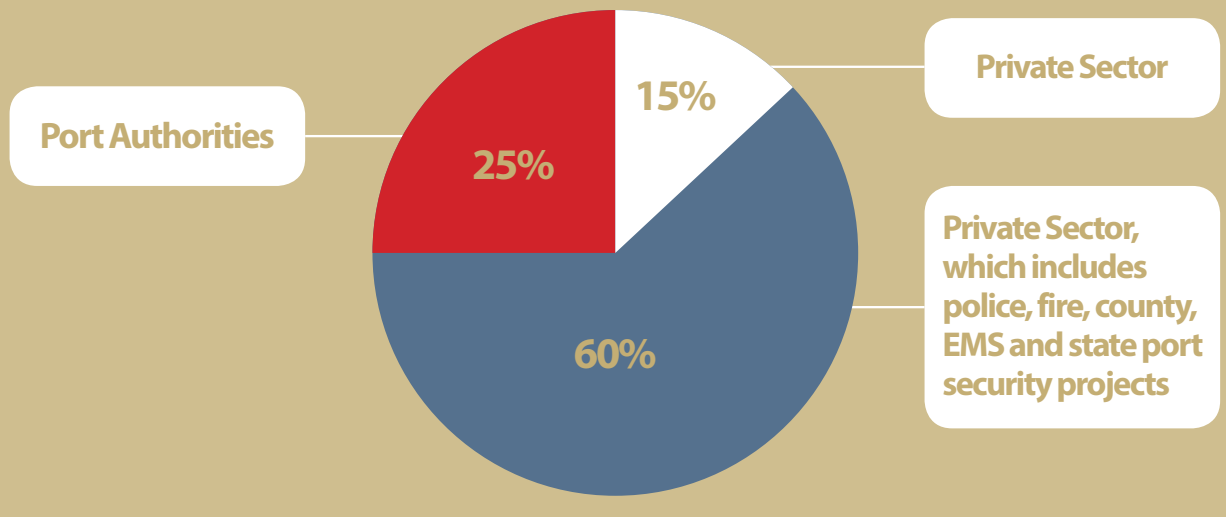
PORTS ARE CENTRAL TO THE SUPPLY CHAIN – IMPORTANCE OF THE PORT SECURITY GRANT PROGRAM

Seaports deliver vital goods and services to consumers, serve as gateways for U.S. exports, create jobs and support local and national economic growth. Seaports are essential economic engines whose cargo activity supports over 23 million American jobs and accounts for over a quarter of the U.S. economy. In 2014, U.S. seaports generated nearly $4.6 trillion in total economic activity.

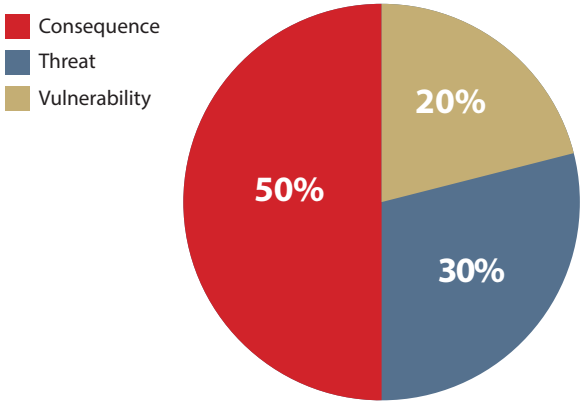
A port authority's operating model varies from port to port. Some ports own and operate cargo terminals, while others lease their equipment and pier space to private operators. Others engage in a combination or hybrid of both activities. Additionally, the types of cargo that move through ports vary widely. Containers, automobiles, energy commodities, break bulk and passengers are a few examples. All port business models have varying security needs; however, the one constant at every port is the commitment to security to ensure the safe movement of all types of cargo and people.

From a security perspective, ports are a place of commerce, business centers within the global supply chain. Ports have multiple access points that make security challenging – be it ship, truck, rail, visitor/employee entrances and increasingly the business networks that are vulnerable to cyberattacks – these access points must be secured. In an interconnected supply chain, security matters. Because of the central role ports play within the supply chain, any disruption or security vulnerability is magnified and has the potential to put in motion a cascading economic disruption that impacts the supply chain and ultimately the national economy.

According to FEMA, funding typically breaks down by percentage in the following categories:



According to FEMA, the risk algorithm breaks down by:



SURVEY SAYS SUSTAINABLE FUNDING FOR THE PORT SECURITY GRANT PROGRAM IS NEEDED

AAPA members identified $4 billion in port security funding needs for U.S. port authorities alone over the next 10 years, which comes to $400 million annually. But the $4 billion in port authority needs is just a small slice of the total potential funding need. AAPA represents 79 U.S ports, and while these port areas are the major freight and passenger access points for the country, there are 281 other ports of varying sizes throughout the country that are also eligible to utilize the PSGP. Within those 361 ports, there are over 3,500 MTSA regulated facilities that continue to have security challenges, such as cybersecurity and other evolving threats, and need funding assistance to properly mitigate the risks.

Furthermore, according to FEMA, over the past 10 years only approximately 25 percent of annual PSGP funding went directly to port authorities. Public sector first responders such as police, fire and emergency management services account for 60 percent of the annual program funding. This means that more is being spent on response capabilities than on awareness, prevention and protection measures. This survey makes the case that after more than a decade, the focus and resources need to revert to public port authorities.

The $4 billion identified by AAPA members is an important starting point for the PSGP, but it does not represent the total need for the program.

HOW THE PORT SECURITY GRANT PROGRAM WORKS

For several years, PSGP funding has been utilized to address security needs outlined in a port's Strategic Risk Management Plan (SRMP). Initially, these plans were blueprints for ports to follow, but they have not been updated in more than a decade. Meanwhile, the threats have evolved.

Furthermore, port security project funding goes through a rigorous local review and national risk evaluation process. Ultimately, each local Captain of the Port (COTP) and their staff provide the final recommendation for their maritime region's project priorities before they are submitted to FEMA. FEMA relies on COTPs to verify PSGP maritime security needs and to rank their region's projects. Primarily, FEMA follows the guidance of the COTP, but as resources have dwindled, FEMA has been unable to fund all COTP-recommended projects.

Once FEMA has received projects lists from each of the 41 COTPs, FEMA runs the projects through a national risk algorithm. The three criteria that make up the risk algorithm are vulnerability, threat and consequences. To determine the final project score, FEMA multiplies the national risk score by the score the COTP gives a project. FEMA funds the highest scoring projects across the country as prioritized by the port areas and as funding permits.

Frequency of Contact with Their Captain of the Port

32% Weekly
27% Monthly
19% Quarterly
11% Daily
7% Semiannually
4% Annually

Maritime Impacted Facilities, Staff and Committees

- MTSA regulated facilities: APPROX. 3,500
- MTSA regulated facilities that require a Coast Guard approved Facility Security Plan: APPROX. 2,500
- COTPs: 41
- AMSCs: 43

Federal partner agencies that participate in the review process include:

- Federal Emergency Management Agency
- Transportation Security Administration
- Maritime Administration

AREA MARITIME SECURITY COMMITTEE

DEFINITION: A federally established forum at all ports for all stakeholders to share information on security issues through regularly scheduled meetings, electronic bulletins on suspicious activities around seaport facilities, and sharing of key documents. The U.S. Coast Guard Captain of the Port (COTP) is authorized to establish and coordinate the Area Maritime Security Committee (AMSC) and appoint members along with other duties as prescribed by regulation. There are 69 AMSCs across the country.

The framework for a collaborative process is in place. The peer review process has been a keystone in FEMA's administering of the PSGP, which coordinates ports, their partners and the localized input of the 43 Area Maritime Security Committees that feed into the 41 COTP zones.

However, the State of Freight IV Port Security Grant Program Report and follow-up conversations with port security grant applicants found that while the level of collaboration, information sharing, and project management is significant and continues throughout the year, ports are not receiving sufficient port security funding.

While collaboration has leveraged some success in funding security projects and coordinating efforts, AAPA security committee members have raised concerns that the PSGP has swayed too far away from "port facility centric" project funding due to expanded eligibility to the program to non-port entities. Ports are the gateways for freight and passengers into the U.S. and are therefore key access points that must be secured just as our land and air borders are.

SUGGESTED PSGP IMPROVEMENTS – BACK TO "PORT-CENTRIC"

AAPA members have advocated that port security grants should be awarded through a port-centric lens. The program veered away from a port-centric approach in the 2007 supplemental bill, which expanded the pool of eligible port applicants to all entities covered by an Area Maritime Security Plan (AMSP).

According to a Government Accountability Office (GAO) report (report #12-47), FEMA implemented key changes to the grant program in the fiscal year 2007 and 2007 supplemental grant rounds to promote enhanced regional collaboration. For instance, in fiscal year 2007, FEMA introduced a tiered

structure to the grant program whereby each port area was placed into a funding group based on risk. FEMA allocated port areas in the highest risk funding group a specific amount of grant funding and grant projects were determined using a regional decision-making process. In the supplemental 2007 grant round, FEMA also transitioned the second highest risk funding group to this collaborative process. The remaining funding groups retained the competitive structure and competed for funding within their funding group. FEMA made two additional changes in the 2007 supplemental funding round to promote regional collaboration. First, FEMA required all Risk Group I and II port areas to select a fiduciary agent to coordinate the grant process in the port area. Second, FEMA required all Risk Group I and II port areas to develop a Port-Wide Risk Mitigation Plan.

"The broadening of port security funding eligibility had massive unintended consequences," said one port executive who was intimately involved with the program at the time and supported opening eligibility. "I fully supported the change at the time, but looking back it diluted the port authority and terminal operator's ability to leverage the program. After 10 years, it's time to revert to a port-centric program."

Since 2007, FEMA has focused funding on anything in a port-wide risk mitigation plan. AAPA believes there is a need to focus funding on the original intent of the PSGP which was focused on the maritime security plans. Prioritizing funding for port authority facilities will achieve this goal.

In follow up to the survey, port security directors have stated that while the PSGP funding process does work, it can be improved by providing more structure to the funding allocation decisions. For example, AAPA recommends that a minimum of 50 percent of the annual PSGP funding be designated within the Notice of Funding Opportunity to be awarded to projects submitted by public port authorities. This process would direct the focus and resources back on public port authorities and be an impetus for increased partnership opportunities between port authorities and maritime stakeholders. Having a baseline investment in public port authorities will provide a starting point for funding decisions, tightening the eligibility for half the program.

Additionally, AAPA recommends that local GFRTs have equal representation of all stakeholder groups including local port authorities and representatives of the container, petrochemical, ferry, cruise or other impacted sectors as appropriate. Protocols should be established within each AMSC so that a member of the GFRT cannot vote or comment on his/her organization's own grant application.

Charles Darwin said, "It is not the strongest of the species that survive, nor the most intelligent, but the one most responsive to change." The same sentiment can be applied to how the country addresses evolving national security trends and more succinctly how we confront our port security and supply chain challenges.

CYBERSECURITY

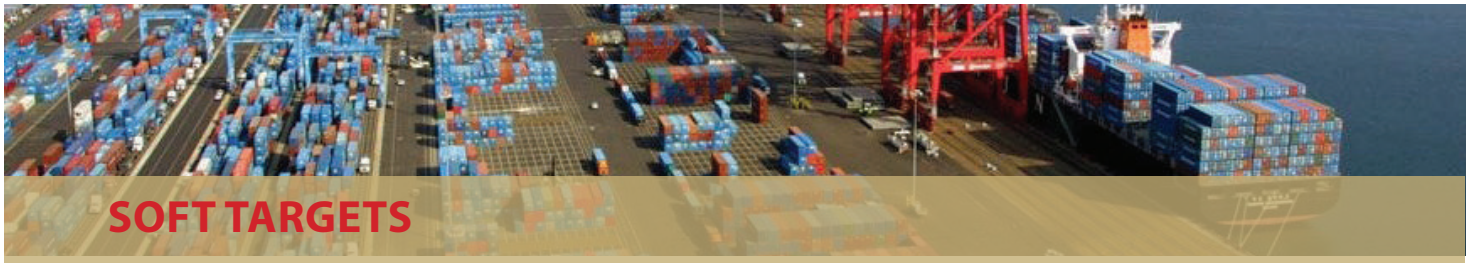
In this survey, 85 percent of AAPA U.S. member ports say they anticipate direct cyber or physical threats to their ports to increase over the next 10 years. Conversely, 10 years ago, cybersecurity, active shooter, drones, increasing energy exports or other soft targets were not highly anticipated threats facing ports and the supply chain.

The 2017 APM Maersk cyberattack illustrated how an incident can start outside the U.S. and have a cascading impact on our ports and terminal operations across the globe. The PSGP program "allows for continual growth of our security regime and the ability to stay ahead of the game as much as possible," said one port security director.

For example, at the Port of Los Angeles, the Cybersecurity Operations Center, which was funded by $2.4 million in PSGP grants, prevents 15-20 million cyber threats on the port's business network each month. However, several survey respondents reported that applications for similar cybersecurity programs in other ports have been denied PSGP funding.

From an industry perspective, 78 percent of ports anticipate using future port security grant funding on cybersecurity, and 90 percent report that future PSGP funding would be used for upgrading technology, such as cameras and other surveillance tools.

In addition, soft targets such as the vulnerability of an active shooter "keep port security staff up at night," said multiple port security directors. In recent years, we have seen active shooters in airports and other infrastructure transfer hubs. Eighty-six percent of ports would use future PSGP funding to enhance physical security, and 65 percent would invest PSGP funding for training to better prepare port and local first responders to respond effectively to soft target threats such as an active shooter,



SOFT TARGETS

DEFINITION: A "soft target" is "a person or thing that is relatively unprotected or vulnerable, especially to military or terrorist attack." Soft targets reflect gaps in a security apparatus that strategically lacks a psychological or physical impediment that would stop or deter an act of harm or incursion. In a maritime setting, port security grants have been utilized to close or eliminate security gaps such as those at cruise terminals to include underwater sonar capabilities and other technologies as necessary.

emergence of high capability drone interception technology and an increased need for waterside security to protect energy transfer stations.

For example, in 2016, Port Everglades utilized PSGP grant funding for a multifaceted active shooter, mass casualty and hostage exercise in which port partners including the Fort Lauderdale-Hollywood International Airport had key roles. PSGP funding will also support a full-scale exercise in 2019 that begins as a vehicle-borne attack at an active cruise terminal and then evolves into an active shooter event. The 2018 grant cycle saw the Broward County Sheriff's Office, in close collaboration with Port Everglades, awarded funding for portable vehicle barriers that can be deployed by one person and stop a large caliber bullet, providing safety and security to both passengers and responders.

MOBILE SECURITY

As the supply chain becomes more integrated, this level of connectivity is likely to expand the direct supply chain outside the gate and increase the need to have mobile security resources. The State of Freight III report noted that 36 percent of ports have direct connections with an inland port. Massport has used PSGP funding with an eye toward securing a growing and expanding supply chain. With the purchase of a portable X-ray system, the port can scan trucks and cars, address bomb threats inside the gate, at terminals and transfer hubs outside the port.

DRONES

While the ground security of ports and the supply chain have been the focus of much of the security of the PSGP, drones are now raising a level of concern. For example, after having implemented a drone permitting requirement in 2017, the Port of Long Beach is experiencing a pronounced increase in the use of drones for commercial activities. As a result, the port is exploring technologies to effectively monitor drone activity over its complex and to identify unmanned aerial vehicles that may pose a safety and security risk.

ENERGY SECURITY

Securing energy commodities continues to be an increasing concern for ports as surging natural gas exports and higher crude oil shipments will help the United States achieve the status of energy exporter for the first time since 1953, according to the U.S. Energy Department.

Port Tampa Bay is investing in securing energy cargo and facilities. Tampa received PSGP funding to purchase a rapid deployable small boat intrusion barrier system to protect a critical petroleum transfer facility. Additionally, small boat attacks against vessels carrying hazardous materials are of major concern to the U.S. Coast Guard and ports. Vessels at berth are especially vulnerable. The Tampa complex serves five different fuel storage facilities critical to the distribution of refined petroleum products in the central Florida region. Upon notification of an impending threat, or the receipt of relevant intelligence regarding a threat against this or similar facilities, the barrier system can be deployed almost immediately, thus securing the vessel in the facility. Traditional water barriers take days to deploy from land and this innovative system can take less than an hour. The barrier system is an example of innovative physical security, made in the USA, that can significantly reduce vulnerability. In this case, Port Tampa Bay used the PSGP funding to create a significant reduction in risk that was not accessible to the port authority through normal funding channels.

INTEROPERABILITY

Traditionally, a project that has maintained continuity among port security partners has been interoperable communication equipment. "Without this equipment we are out there alone," said one port security director. Ports such as Port Fourchon rely on the PSGP so that they can upgrade their interoperable communication capabilities to communicate with their local, regional and state law enforcement partners along the Gulf Coast.

PORT-WIDE MARITIME DOMAIN AWARENESS

Port-wide maritime domain awareness consists of security operating systems that connect and integrate video feeds, radar, weather and law enforcement data into a single platform. These operating platforms provide the baseline for port security and communications systems in and around maritime facilitates. Ports and the PSGP have invested in these systems throughout the life of the program. With new technology coming online, increasing cyber threats and more integrated communication systems, upgrades in many ports must be made. These security operating platforms are essential to the security of maritime facilities and will continue to be in the coming decade. Funding for upgrading these systems must be a priority.

A GROWING SUPPLY CHAIN AND GROWING PORT SECURITY CONCERNS

Increasingly, when freight infrastructure investment is planned, supply chain security is also involved. In 2016, the Fixing America's Surface Transportation (FAST) Act created a funded freight program, which includes ports as eligible recipients. Ports are now firmly recognized as part of the surface transportation, logistics and distribution network. Equally important, the FAST Act required states to complete state freight plans to continue to receive their freight formula funding. The results have been impressive. To date, 90 percent of the states have submitted multimodal state freight plans to the U.S. Department of Transportation. This is important because it signals that states recognize the value of multimodal projects, but also that the supply chain is operational and ports are at the center of this activity.

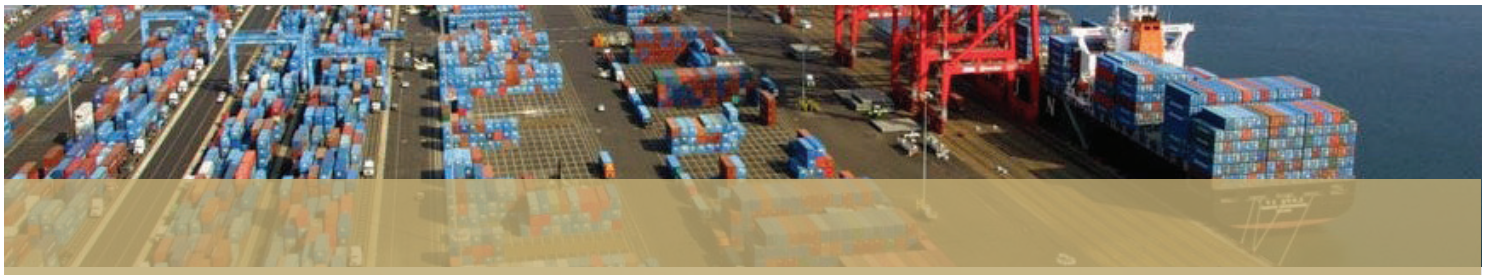
The way the nation moves freight, protects cargo, purchases items, communicates and integrates new technology into security has transformed the supply chain landscape post-9/11. In 2001, there was no Amazon as we know it today (it was a bookstore), no daily discussions on cybersecurity, no iPhones, only the beginnings of modern e-commerce. Now, anyone with a smart phone can be a shipper or consumer. The supply chain now carries more value with more access points.

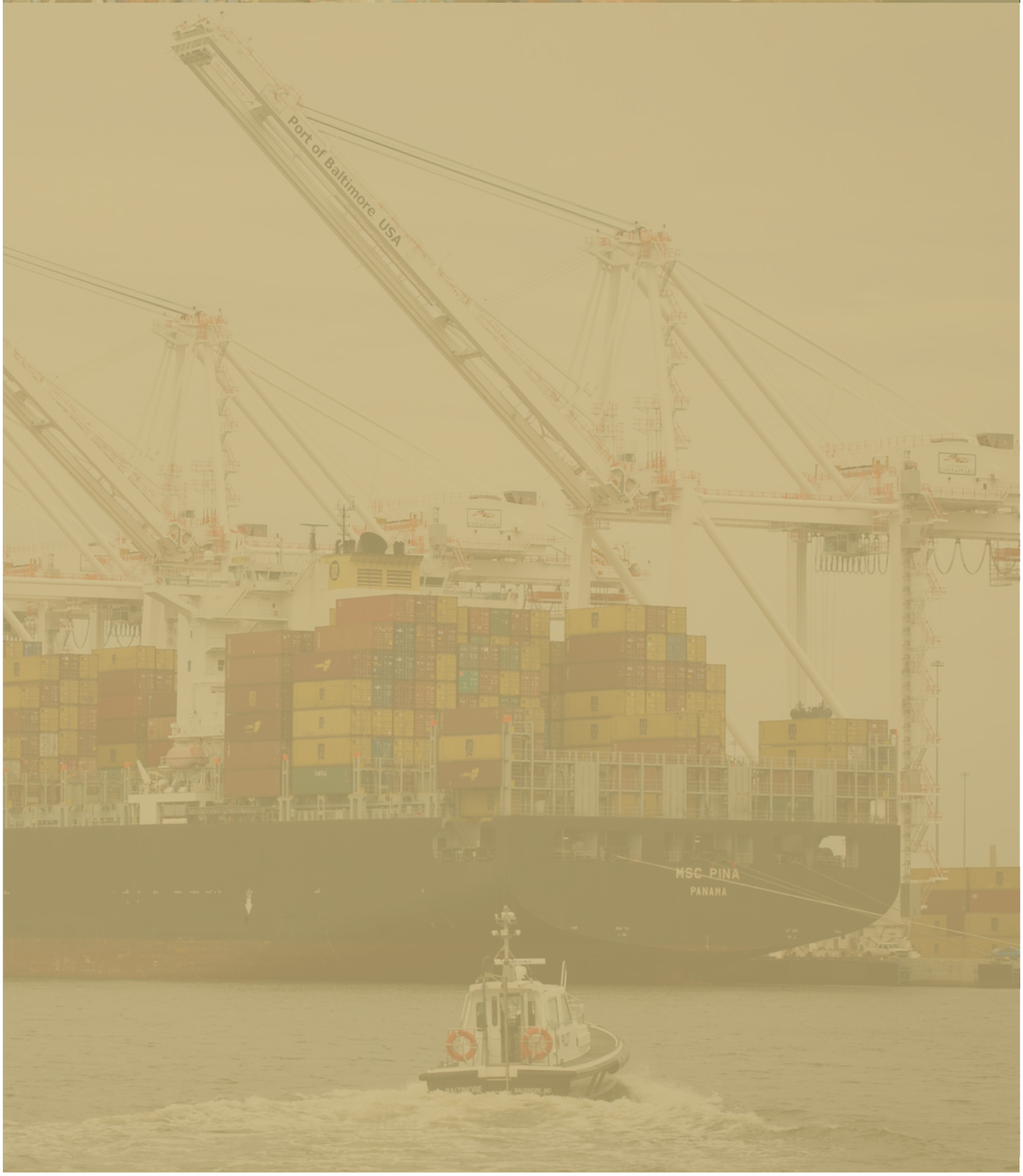
Port security directors now report that supply chain security is a major concern and flash point for the overall security of a port. Assuming multiple roles, the nation relies on the PSGP to protect ports, communities and growing value of the supply chain. According to the U.S. Census Bureau, the U.S. merchandise trade value increased 70.2 percent between 2004 and 2017. As America's freight network is built out and the supply chain becomes more integrated and operational, ports are often the first – and sometimes the last – line of defense.

CONCLUSION

Ports have always been a critical node in the supply chain, no matter how they structure their operations or what kinds of cargo they handle. Securing port facilities to ensure safe and reliable goods movement is critical to the nation's economic success. Meeting today's security threats requires flexibility and adaptation on behalf of ports authorities and their partners, who continue to confront evolving challenges.

Keeping ports secure and the supply chain moving also requires a renewed commitment from the federal government regarding the funding levels and strategic direction of the PSGP. AAPA member port authorities identified $3.89 billion in needs in the next ten years to maintain and upgrade their facilities and ensure that they are well-equipped to address new security challenges. Providing adequate funding and refocusing the PSGP to become more port-centric, the federal government can demonstrate its commitment to the security aspect of the nation's supply chain.




Port of Baltimore USA
MSC PINA
PANAMA

@AAPA_Seaports

@seaportsdeliverposperity

American Association of Port Authorities

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

1010 DUKE STREET | ALEXANDRIA, VA | 22314-3589

703.684.5700 | FAX: 703.684.6321 | AAPA-PORTS.ORG