The Port of
LONG BEACH

The Written Statement of
Mario Cordero
Executive Director
Port of Long Beach

Before the
House Committee on Homeland Security
United States Congress

"Examining Physical Security and
Cyber Security at Our Nation's Ports"
October 30, 2017

Port of Long Beach
4801 Airport Plaza Drive
Long Beach, CA 90815

INTRODUCTION

Thank you, Chairman McCaul and members of the House Homeland Security Committee for the opportunity to speak on the subject of port security including; cargo screening, cyber security and industry partnerships in the maritime environment. My name is Mario Cordero and I am the Executive Director for the Port of Long Beach. Prior to joining the Port as the Executive Director, I served as Chairman of the Federal Maritime Commission and before that I served as a Long Beach Harbor Commissioner.

BACKGROUND

As the second busiest seaport in the United States, the Port of Long Beach is a major gateway for U.S.-Asia trade and a recognized leader in security. The Port is an innovative provider of state-of-the-art seaport facilities and services that enhance economic vitality, support jobs and improve the quality of life and the environment. As a major economic force, the Port supports more than 30,000 jobs in Long Beach, 316,000 jobs throughout Southern California and 1.4 million jobs throughout the United States. In 2016, the Port of Long Beach moved more than 6.8 million twenty-foot equivalent units (TEUs) of cargo, also known as containers. The Port's cargo containers account for nearly 33 percent of the containers moving through U.S. West Coast ports, and nearly 1 in 5 moving through all U.S. ports. Currently, the Port is on pace for a 7 percent growth for 2017.

Combined with the Port of Los Angeles, both ports comprise the San Pedro Bay, the busiest port complex in the nation and the ninth-busiest port complex in the world. Together, the two ports moved $400 billion in containerized trade or nearly 16 million TEUs in 2016. This includes almost 40 percent of the nation's imported cargo. A 2010 report commissioned by both ports and the Alameda Corridor Transportation Authority found that cargo moving through the San Pedro Bay Port Complex, made its way to every Congressional district in the continental United States. As a result of the volume of cargo moved through this complex and transportation-related activities, protecting the San Pedro Bay ports is vital to our national economy.

PORT SECURITY

Safety and security are among the top priorities at the Port of Long Beach. Since the terror attacks of September 11, 2001, the Port has received more than $1.6 billion in federal grants to complement the extensive investments made by the Port, the City of Long Beach, marine terminal operators and carriers to ensure the nation's largest container gateway remains open and safe.

The Port of Long Beach's Security Division collaborates regularly with the Federal Bureau of Investigation (FBI), U.S. Customs and Border Protection (CBP), U.S. Coast Guard (USCG), the Long Beach Police and Fire departments, as well as other federal and state law enforcement, security, and emergency-response agencies. Ensuring the security of major international gateways like the Port of Long Beach is a multilayered

security effort that requires the continued participation of and funding by federal partners. Since 2001, we have responded to evolving threats to the integrity of the Port, threats that now include cyber-attacks. In addition, a threat that also has real potential for damage or disruptions is from unmanned aerial systems.

The Port takes a leadership role in the development of strategies to mitigate security risks in the San Pedro Bay, working closely with multiple partners, both public and private, to plan and coordinate security measures. Based on our professional experience, we recognize threats and formulate the best mitigation strategies. The Port of Long Beach's Joint Command and Control Center, a 24-hour a day maritime domain awareness center, is a critical hub for coordinated security efforts that include partnerships with local, state and federal law enforcement agencies as well as maritime and private sector stakeholders. Formalized agreements have been made with these partners to share security information, coordinate threat information, develop plans and coordinate operations.

The Control Center houses over $100 million in technical security assets. Through innovative efforts, the Port has a monitoring network of over 400 cameras, a comprehensive fiber-optic network, a port-wide wireless system, an integrated security management system for synchronized monitoring and quick threat detection, access control and alarm monitoring, boat patrols, radar systems, a vessel tracking system, and sonar equipment. In addition, law enforcement operations have been fully integrated between the Port of Long Beach Harbor Patrol and the Long Beach Police Department.

Cargo Screening

Securing the flow of goods to and from the United States is a complex mission, involving governments, businesses, and non-profit organizations across the globe. And, the Port of Long Beach represents a key player in this mission. Together with these partners, the Port seeks to secure the global supply chain through a broad range of tools including information-sharing, risk-based analytics, and the application of advanced technologies. While we understand Congressional interest in 100 percent scanning of all incoming cargo at our nation's ports, to do so would impede the flow of commerce to a halt and require an unprecedented investment in technology and personnel at each of the hundreds of terminals across the nation. A greater return on investment can be made by deepening the level of engagement with global partners and utilizing 'big data" to target those containers that pose a concern. The Port strongly recommends continuing to invest in programs such as Custom's Trade Partnership Against Terrorism that incentivize shippers to secure each step in the supply chain, rather than focusing on a single step in the process.

As it relates to "big data", the Port is actively working with federal partners to tap into their targeting capabilities to provide a coordinated response to vessels and cargos of interest. The Port of Long Beach is extending these layers of protection landside by developing analytics and sensors to better forecast the landside movement of goods to and from the port. This will not only better align Port personnel and security

infrastructure deployments, it also improves the efficiency of our local and intermodal operations. These efforts have been achieved by investments from the Port and the Port Security Grant Program (PSGP). Reductions to the PSGP has placed constraints on the ability of ports around the nation to sustain these investments and it is recommended that Congress restore the Port Security Grant Program to the $400 million level so that U.S. ports can continue to stay one step ahead of adversaries.

Cyber Security

Information Technology Risk and Cyber Security

The number of U.S. data breaches across educational institutions, shipping firms, government agencies, military, medical facilities, financial firms and other businesses jumped to a record to a record 791 in the first 6 months of 2017. This is a 29 percent increase from the same time period in 2016. Information technology is a critical component of the goods movement system. The Port is tightly integrated with various stakeholders across the supply chain and it is essential that data exchanged between stakeholders is protected.

Phishing campaigns targeting general port staff and stakeholders have increased by up to 70 percent throughout the nation. Cyber-attacks are increasingly targeting the sectors of the economy that have traditionally underspent in the information management and technology areas. For both the private and public sectors, it is a matter of when, not if, a cyber-attack will take place.

The Port of Long Beach's Information Management Division successfully thwarts over 30,000,000 threats a month. The goal is to build a sustainable program that balances the need to protect against cyber-attacks while balancing the need to run the Port's business. In this information era, new technologies are outpacing traditional information security controls.

Maritime Sector Application

The Port of Long Beach relies heavily on information technology to operate, as well as to secure the port complex and its assets. Like other industries, the maritime sector has seen an increase in cyber-attacks, in part because ports are national economic drivers and manage critical infrastructure. That is why, in addition to above water, on water, and underwater security monitoring and threat detection, cyber security has become a critical endeavor for the Port.

Private sector businesses, such as terminal operators, control a substantial portion of the Port's economic activity through a wide variety of facilities. In the port complex, the targets for major cyber threats include; port administration facilities, shippers, vessels, terminal operating systems, equipment, storage facilities, rail, and truck operations. Potential perpetrators who could carry out cyber-attacks include state-sponsored criminal groups and individuals, either inadvertent or intentional. Cyber threats to the

maritime environment include; hacking, jamming, phishing, spoofing, malicious programs, taking control and network denial of service.

Some of the motivating factors for cyber criminal activities may involve smuggling, cyber extortion, gaining business advantage, intellectual property theft, and disrupting or destroying critical national infrastructure. In addition to manmade cyber threats, the maritime sector is also susceptible to technology disruption from natural hazards such as earthquakes, hurricanes and tsunamis. Threats to ports and their partners are dangerous to the large number of workers, travelers, and visitors in and around the port community. Coupled with the potential catastrophic economic impacts, maritime cyber events could impact our national well-being as much as, if not more than, other types of attacks.

Business resiliency has become a critical part of the Port's ongoing cyber security planning. Reducing the potential for single-point failure, building redundancy into technology systems, and system recovery back-up processes are vital to ensuring ports remain viable and resume operations as swiftly as possible in the event of an incident.

Response and recovery are critical to successful mitigation and business resumption. Protocols must be clear on how to best contain an incident to prevent further interruption, and response teams must have specialized training and be prepared to engage 24/7. Protocols should make clear who receives notice of the event and what assets are available to quickly assist. In a port environment, a resilient logistics chain needs to be able to absorb a business interruption and then quickly resume an acceptable level of goods movement. In order to develop a comprehensive resiliency plan to address cyber security, factors that should be addressed include; infrastructure needs and protection, transportation systems, and development of business continuity plans.

Addressing Challenges

There are a number of challenges that must be addressed to enhance cyber security in maritime environments. There is not a one-size-fits-all solution because each port has a different business model. A lack of awareness about an organization's own systems creates opportunities for exploitation at a basic level. Information technology systems can be a patchwork of legacy structures, some integrated with newer technologies. These systems can be administered by operators with a myopic focus resulting in the "siloing" effect. The "siloing" effect is not an information technology problem. It is an organizational and cultural issue that takes effort to change. At the Port of Long Beach, there is an ongoing effort to align the enterprise Information Management function with the special needs of the Security Division.

The Port of Long Beach's Information Management Division has developed and implemented a well-received enterprise-wide online cyber security awareness training program. Best practices show that information security requires shaping appropriate behavior in people as well as making sure funding is allocated at the appropriate level

for rapid detection and response approaches. It is expected that by 2020, 60 percent of enterprises, information security budgets will be allocated for rapid detection and response approaches, up from less than 30 percent in 2016.

Solutions

Solutions to these cyber security challenges exist. All entities must take inventory and identify their own systems and capabilities, which includes identifying employee and contractor access to port facilities and information systems. In assessing impacts, it has been determined that people cause the most damage. The Port of Long Beach has taken a leadership role in having implemented extensive cyber security awareness Some terminal operator stakeholders have requested that the Port aid them in developing similar programs. It is believed that once cyber operations are understood on an enterprise level, systems and protocols can be organized to continuously promote cyber security throughout the organization. Legacy systems can be evaluated and updated to meet the ever-changing cyber security needs.

The next step in achieving awareness is to have a comprehensive vulnerability assessment conducted by subject matter experts. It is critical to identify and prioritize gaps that could lead to interruptions affecting key operations. The Port of Long Beach has undergone regular assessments over the last several years from well respected partners and plans on continuing this practice. The governance of a comprehensive enterprise wide cyber security program that is integrated into a larger stakeholder framework continues to be one of our key information technology goals.

When a cyber-attack occurs, decisions must be driven by information. An environment that promotes the sharing of information will include balancing the need to protect propriety information with protecting our national critical infrastructures. The City of Los Angeles created a Cyber Security Fusion Center to facilitate the exchange of cyber information, and the ports of Long Beach and Los Angeles both have access. The Port of Long Beach takes pride in being led by our Information Management Division in being recognized as National Cyber Security Alliance – Cyber Security Champion since 2010.

The Port also participates in the San Pedro Bay Cyber Working Group and the Critical Infrastructure Partnership Advisory Council. The USCG Sector Los Angeles/Long Beach, Area Maritime Security Committee has approved a Cyber Security Subcommittee and we are active participants and the Information Technology function provided a presentation on the latest information on proactively preventing cyberattacks. This information was shared with everyone and provided to the USCG leader for inclusion in the ongoing sharing efforts. In 2016, the Port of Long Beach staff participated in Cyber Guard 16, a national level cyber security exercise sponsored by Department of Defense, Department of Homeland Security and FBI. As cyber threats cross traditional physical and jurisdictional boundaries, we support the involvement of state, local and private stakeholders in a comprehensive, national-level exercise program.

The USCG's focus on cyber security in the maritime sector has created a need for specialized mission requirements. These requirements must be supported through adequate funding to develop and acquire subject matter experts and other resources to deliver meaningful guidance to ports around the country. Valuable guidance has been provided by the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cyber Security. Coordination between NIST and the USCG will continue to lead the way in formulating the strategies required for a more comprehensive national cyber security posture. There should not be one-size-fits-all approach to managing cyber security risk because each port or logistics partner will experience different threats and vulnerabilities, as well as have different capabilities to address them.

UNMANNED AERIAL SYSTEMS

The Port of Long Beach is also actively following the discussion of incorporating Unmanned Aerial Systems (UAS) into the national airspace. While the Federal Aviation Administration (FAA) Extension, Safety, and Security Act called for enforcing regulations to allow operators of critical national infrastructure to apply to prohibit or restrict UAS operation adjacent to these facilities, no such rule was promulgated. Enacting this legislation is crucial to the safety of those who work in the port complex. The UAS industry has quickly outpaced the federal rulemaking process. The unhindered operation of UAS's near terminals and ships could pose an immediate danger. UAS operations in areas where they present an inherent danger must be restricted and first responders should be deemed the enforcement entity authorized to mitigate threats.

The Port of Long Beach's Board of Harbor Commissioners recently approved a UAS permitting and enforcement mechanism, but based upon current case law citing federal preemption, the Port is limited to only regulating the take-off and landing. As a result, we are supportive of the language added to the FAA Reauthorization Act of 2017 to further study the potential gaps between existing federal, state and local laws. A review of the time it will take to develop a comprehensive look at the full range of local efforts and juxtapose them against the ever-evolving federal authorities could take years. Port staff has also identified significant gaps between what the FAA can enforce and where local enforcement can act. The FAA appears to have a limited footprint in the field and cannot respond to reports of UAS flying near critical infrastructure or in a careless and reckless manner. It is believed that this type of enforcement is better delegated to local public safety personnel, working in conjunction with their federal partners.

CONCLUSION

It is important to recognize that while we vigorously try, no one can stop all attacks. It's a matter of when, not if and being prepared with a response plan that involved both technology and information recovery as well as making sure this is integrated into our Business Continuity program. Protecting U.S. ports must be a core capability of our nation. There seems to be either high-level discussion about cyber security or fragmented tactical level technical detail. Focusing on the development of common

frameworks and strategic policies is sorely needed. A roadmap that provides guidance and flexibility for industry decisions makes sense and will strengthen our national cyber security posture.

Thank you again for the opportunity to address the Committee on these critical issues. The Port of Long Beach stands ready to work with you and your staff to help protect the people and economic vitality of the United States.