THE PORT
OF LOS ANGELES

WRITTEN TESTIMONY

OF

EUGENE D. SEROKA

EXECUTIVE DIRECTOR

THE PORT OF LOS ANGELES

ON

EXAMINING PHYSICAL SECURITY AND CYBERSECURITY AT OUR NATION'S PORTS

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON HOMELAND SECURITY

OCTOBER 30, 2017

The Port of Los Angeles
Eugene D. Seroka
Written Testimony
October 30, 2017

EXAMINING PHYSICAL SECURITY AND CYBERSECURITY AT OUR NATION'S PORTS

Chairman McCaul, Ranking Member Thompson and Members of the House Homeland Security Committee:

I'm Gene Seroka, Executive Director of the Port of Los Angeles, and on behalf of our Board of Harbor Commissioners and the men and women who work in our port complex, it is my pleasure to welcome you to America's Port. I appreciate this opportunity to testify before you today and play a role in shaping a critical area of need in the maritime shipping community. With respect to our physical security and cybersecurity preparedness the Port takes its responsibilities seriously and has a robust security and emergency preparedness plan to prevent and manage either natural or man-made disasters.

In order to protect our Port, we created and continue to expand the capabilities of a security infrastructure that fully integrates both physical and cybersecurity preparedness throughout the port complex, and supports coordinated rapid response with law enforcement agencies. Our infrastructure connects port-wide surveillance systems, and integrates a variety of measures including access control, communications, and intrusion detection systems. Recognizing the magnitude of the task of securing our gateway, we have invested hundreds of millions of dollars of our own funds in our security infrastructure. At the same time, finding opportunities for assistance from federal grants is paramount and an area where we continue to look for support from Congress. Regarding our level of coordination with law enforcement, as demonstrated earlier today on your various site visits, the Port works hand in hand with local law enforcement agencies, our state partners, and our federal partners – including the U.S. Coast Guard (USCG), the U.S. Customs and Border Protection (CBP), the Federal Bureau of Investigation (FBI), the U.S. Secret Service, and the U.S. Department of Homeland Security (DHS).

The Port of Los Angeles is especially sensitive to the needs for cybersecurity protection because we believe the maritime shipping industry, while already having integrated technology throughout the system, is becoming increasingly reliant on digital industrial infrastructure.

Last year, we partnered with GE Transportation to develop a first-of-its-kind port visibility tool that allows our supply chain partners – from the cargo owners to the liner shipping companies and everyone involved with the cargo conveyance process – to achieve more efficient operations through secure, channeled access to big data. Earlier this year, we piloted the tool at our largest terminal with tremendous assistance from U.S. Customs and Border Protection. The success of the pilot has encouraged us to expand the portal to the rest of our terminals.

While the digitization of the maritime supply chain is an exciting opportunity, earlier this year, we also saw the vulnerabilities associated with application of digital infrastructure to our operations. In June, the information systems of one of our industries largest companies, Maersk, was compromised by a cyberattack. The global cybersecurity attack called "non-Petya" severely impacted Maersk's operations, both globally and at the Port. The reverberations of that attack were felt here at the Port of Los Angeles, where one of largest terminals shut down out of an abundance of caution. Recent reports indicated the incident cost Maersk over $300 million. This incident, coupled with the increasing reliance on digital infrastructure, should be a "call to arms" for the industry.

We applaud you, Mr. Chairman and Ranking Member, for your leadership on the passage of the Cybersecurity Information Sharing Act (CISA) in 2015. We also want to acknowledge the work of Congressmembers Torres, Correa, and Barragán, all of whom are here with us today, along with their other co-sponsors, for all of their work on the recent House passage of H.R. 3101, "Strengthening Cybersecurity Information Sharing and Coordination in our Ports Act of 2017." We support that legislation and believe that cybersecurity information sharing is a key tool to help protect our ports and maritime community against cybersecurity attacks.

Furthermore, we appreciate the partnership with the U.S. Coast Guard (USCG) and have worked collaboratively with them for many years. We appreciate the guidance issued in December 2016 to clarify the reporting of suspicious activities and breaches of security to include cybersecurity. We believe the Maritime Transportation Safety Act (MTSA) addresses the key risks to the industry and that it can be flexible enough to manage cybersecurity risks as well as others in the industry. At the same time, the USCG issued a notice for comment in July, the draft Navigation and Inspection Circular (NVIC) Guidelines for Cyber Risks at MTSA regulated facilities which provided guidance on how cybersecurity risks should be integrated into Facility Security Assessments (FSAs).

Among ports, we at the Port of Los Angeles have worked to be a leader on cybersecurity issues for many years. We built and created a comprehensive Cyber Security Operations Center (Center) that has been operational since 2014 – the first of its kind for any U.S. port. The Center plays an invaluable role for the Port and is managing an unprecedented level of attacks: over 20-million cyber intrusion attempts per month, literally seven-to-eight attacks every second on average. The Port is seeing a growing volume and variety of malicious cyberattacks ranging from denial-of-service attacks, more standard data breaches, botnet and malware attacks along with possible insider threats.

The Center is literally the centerpiece of our cyber security operation. It is run by a dedicated cybersecurity team and is used as a centralized location to proactively monitor network traffic to prevent and detect cyber incidents. It is also able to contain and manage any attacks that can then be discussed with law enforcement as needed for investigation purposes. It uses advanced systems to proactively monitor and prevent, detect and respond to cyber-attacks. It also collects data that can be analyzed and shared with other agencies, such as the FBI, the U.S. Secret Service and local law enforcement.

Partial funding for the development of the Center came through the Port Security Grant Program with the majority of the funds coming from the Port. It is ISO 27001 certified, the recipient of American Association of Port Authorities IT Awards of Excellence in 2014 and 2016, and has been featured in several nationwide publications. The Port of Los Angeles is the only U.S. port authority with an ISO 27001 certified Cyber Security Operations Center. However, our work is far from finished – much more needs to be done.

To that point, while the Port is working to manage its own systems, we know that there is cross-sector risk that comes from all of the players in the Port environment. As mentioned, the Port environment is one where we are seeing increasing digitization; so it is critical that cybersecurity be imbedded in the front end – ensuring there is “security by design” in the process. As you might imagine, the port ecosystem is a complicated one, relying on vendors, supply chain providers, the multitude of clients and service providers. To add another layer of complexity, the Port also relies on other Critical Infrastructure (CI) providers like the energy, communications and information technology sectors as well. In many cases, the Port may not have visibility into any of these partners or other CI sectors cybersecurity posture, and as a result, cyber risk exists throughout that system. In light of the constantly rising cybersecurity attacks and

systemic risks to the maritime sector, it is critical that the port and maritime community come together to discuss the shared risk and tools to approach the risk. To that end, we would recommend a number of policy initiatives for review and consideration together:

1. Create a seamless effort between the U.S. Coast Guard and the National Program and Protection Directorate (NPPD) at the U.S. Department of Homeland Security to help the maritime industry break down and share best practices to manage cybersecurity risk from the operational impacts on a cyber-attack to the more traditional data breach attacks.

2. Continue efforts working with the maritime sector so we better understand how to assign roles and responsibilities to the multiple players in the cybersecurity world, including the USCG, NPPD, FBI, Secret Service, law enforcement etc.

3. Run National Level Exercises that include cybersecurity attacks on the maritime sector to better inform and focus the need for cybersecurity vulnerability assessments, preparing cyber incident response plans, and other basic cyber planning and response exercises.

4. Incentivize cybersecurity project applications to the Port Security Grant Program funding programs; waive the cost-share requirements for cybersecurity assessments at major trade gateways, and maintain the Port Security Grant Program funding level at $100 million.

5. There is a need for increased CBP maritime staffing to ensure the security of passenger and freight facilities, and there is a need for CBP detection equipment to be upgraded to ensure new technologies are utilized to detect security risks and provide cybersecurity safeguards at major port gateways.

6. Work to evaluate the current status of existing maritime Information Sharing and Analysis Centers (ISAC) to measure the effectiveness and value of maritime only ISACs.

7. Expand engagement with the International Maritime Organization (IMO) and other applicable international organizations to increase global maritime cybersecurity awareness, preparedness, and response standards.

The Port of Los Angeles is the largest container port in the country and an important economic driver for the nation. U.S. seaports need to remain a high priority when

determining projects to enhance our country's position in the global trade market. In order to compete in the international marketplace, our facilities and infrastructure needs to be maintained at the highest level with continued federal investment.

The Port of Los Angeles would like to thank the Committee for holding this hearing as the importance of this topic cannot be understated. Our nation's ports cannot be forgotten when security is at the forefront of maintaining our national economy.

The Port of Los Angeles takes a great deal of pride in being a model for port security infrastructure. We trust that Congress will take the necessary action to ensure that the Port of Los Angeles and ports across the country receive the necessary funding to continue to make infrastructure improvements. With the proper focus on security infrastructure, the United States will continue to lead the world in international trade well into the twenty-first century.

###