AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

EXAMINING PHYSICAL SECURITY AND CYBERSECURITY AT OUR NATION'S PORTS

FIELD HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

OCTOBER 30, 2017

Serial No. 115–35

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

28–822 PDF WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
JOHN KATKO, New York
WILL HURD, Texas
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
CLAY HIGGINS, Louisiana
JOHN H. RUTHERFORD, Florida
THOMAS A. GARRETT, JR., Virginia
BRIAN K. FITZPATRICK, Pennsylvania
RON ESTES, Kansas
VACANCY

BENNIE G. THOMPSON, Mississippi
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California

BRENDAN P. SHIELDS, *Staff Director*
STEVEN S. GIAIER, *Deputy General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
HOPE GOINS, *Minority Staff Director*

CONTENTS

Page

STATEMENTS

The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Chairman, Committee on Homeland Security:
Oral Statement 1
Prepared Statement 2
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Oral Statement 3
Prepared Statement 5

WITNESSES

Rear Admiral Todd A. Sokalzuk, Commander, Eleventh Coast Guard District, U.S. Coast Guard, U.S. Department of Homeland Security:
Oral Statement 6
Prepared Statement 7
Mr. Carlos C. Martel, Director of Field Operations, Los Angeles Field Office, U.S. Customs and Border Protection, U.S. Department of Homeland Security:
Oral Statement 9
Prepared Statement 11
Mr. Eugene D. Seroka, Executive Director, The Port of Los Angeles:
Oral Statement 15
Prepared Statement 17
Mr. Mario Cordero, Executive Director, The Port of Long Beach:
Oral Statement 19
Prepared Statement 21
Mr. Ray Familathe, International Vice President, International Longshore and Warehouse Union:
Oral Statement 25
Prepared Statement 27

FOR THE RECORD

The Honorable Nanette Diaz Barragán, a Representative in Congress From the State of California:
Comments 38
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Statement of Anthony M. Reardon, National President, National Treasury Employees Union 52

APPENDIX

The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Chairman, Committee on Homeland Security:
Letter From the National Association of Waterfront Employers 55

EXAMINING PHYSICAL SECURITY AND CYBERSECURITY AT OUR NATION'S PORTS

Monday, October 30, 2017

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
San Pedro, CA.

The committee met, pursuant to notice, at 1 p.m., at the Port of Los Angeles Administration Building, 425 South Palos Verdes Street, San Pedro, California, Hon. Michael T. McCaul (Chairman of the committee) presiding.

Present: Representatives Thompson, Correa, and Barragán.

Also present: Representatives Estes, Rohrabacher, Hunter, Lowenthal, and Torres.

Chairman MCCAUL. The Committee on Homeland Security will come to order.

Committee's meeting today is "Examining the Physical Security and Cybersecurity of Our Nation's Ports."

Before I begin, I would like to note that we have a number of Members that are not on the Committee of Homeland Security attending today. I would ask unanimous consent that they be allowed to participate in today's hearing.

I appreciate the effort taken on behalf of all those involved to have this important field hearing take place. I want to thank the Port of Los Angeles for hosting us.

This is an official Congressional hearing. So we must abide by certain rules of the Committee on Homeland Security and the House of Representatives.

I kindly wish to remind our guests today that demonstrations from the audience, including applause and verbal outbursts, which I doubt will happen here today, will be a violation of House rules.

It is important that we respect decorum and rules of the committee.

I have also been requested to state that photography and cameras are limited to accredited press only.

I now recognize myself for an opening statement.

Today Members of our committee have gathered here to examine the physical and cybersecurity of our Nation's ports. I would like to thank everyone who has traveled a great distance to be here and to CBP and the Coast Guard for the tour of Port of Los Angeles and the Port of Long Beach.

I would also like to thank each of the witnesses and look forward to hearing your thoughts on how we can work together to strengthen the security of America's ports.

America's port system is an industrial engine that drives much of our economic success. Currently, U.S. seaports support 23 million American jobs and 4.6 trillion in economic activity, or 26 percent of our economy.

This year alone, the Port of Los Angeles has processed over 6 million containers. These ports will only continue to remain busy, as our trade volume is expected to quadruple by 2030.

A safe and unrestricted flow of goods and services through our marine transportation system has allowed the United States to become a global economic superpower.

Keeping our ports and our cargo containers safe is absolutely vital to our Homeland Security as well as our National financial health. We must make sure they are not susceptible to attacks from our enemies.

Unfortunately, America's adversaries are constantly looking for ways to strike our country with cyber attacks. As our port systems increasingly benefit from new technology and advanced computer systems, they also find themselves in the crosshairs of international hackers and rogue nation-states.

In June, this very port was briefly shut down because of a cyber attack that cost nearly $300 million in economic damage. That is not acceptable. We must do more to strengthen cybersecurity and these essential maritime hubs.

Fortunately, the Committee on Homeland Security has been taking action. Proud to say that we have a great track record when it comes to work across party lines to pass common-sense legislation.

Last Monday, the House passed a reauthorization of the Customs Trade Partnership Against Terrorism program, an important public/private-sector partnership that strengthens cargo security and international supply chains.

That very next day, we passed legislation that requires the Secretary of DHS to implement a risk assessment model which focuses on cybersecurity vulnerabilities and risks at America's ports.

In July, Republicans and Democrats came together to pass the first ever comprehensive reauthorization of DHS with an overwhelming bipartisan vote. This reauthorization approves the preparedness and readiness capabilities of the Coast Guard and TSA while creating a mechanism for port operators to share cyber threat information and best practices.

Chairs of the 9/11 Commission, Tom Kean, Lee Hamilton, have recently called on the Senate to pass this reauthorization. It needs to get to the President's desk and signed into law.

Finally, I would like to express the committee's appreciation to the leadership and staff of the Port of Los Angeles Harbor Administration for making this event possible.

[The statement of Chairman McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

OCTOBER 30, 2017

Today, Members of our committee have gathered here to examine the physical security and cybersecurity of our Nation's ports.

Before we begin however, I would like to thank everyone who has traveled a great distance to be here and to CBP and the Coast Guard for the tour of the Port of Los Angeles and the Port of Long Beach.

I would also like to thank each of the witnesses and I look forward to hearing your thoughts on how we can work together to strengthen the security of America's ports.

America's port system is an industrial engine that drives much of our economic success. Currently, U.S. seaports support 23 million American jobs and $4.6 trillion in economic activity, or 26% of our economy.

This year alone, the Port of Los Angeles has processed over 6 million containers. These ports will only continue to remain busy, as our trade volume is expected to quadruple by 2030.

A safe and unrestricted flow of goods and services through our marine transportation system has allowed the United States to become a global, economic super power.

Keeping our ports and our cargo containers safe, is absolutely vital to our homeland security as well as our National financial health. We must make sure they are not susceptible to attacks from our enemies.

Unfortunately, America's adversaries are constantly looking for ways to strike our country with cyber attacks.

As our port systems increasingly benefit from new technology and advanced computer systems, they also find themselves in the crosshairs of international hackers and rogue nation states.

In June, this very port was briefly shut down because of a cyber attack that cost nearly $300 million in economic damage. That is not acceptable.

We must do more to strengthen cybersecurity of these essential maritime hubs.

Fortunately, the Committee on Homeland Security in the House has been taking action. And I am proud to say that we have a great track record of working across party lines to pass common-sense legislation.

Just last Monday, the House passed a reauthorization of the Customs Trade Partnership Against Terrorism (C–TPAT) program, an important public-/private-sector partnership that strengthens cargo security and international supply chains. The very next day, we passed legislation that requires the Secretary of DHS to implement a risk assessment model which focuses on cybersecurity vulnerabilities and risks at America's ports.

In July, Republicans and Democrats came together to pass the first-ever, comprehensive reauthorization of DHS with an overwhelming bipartisan vote. This reauthorization improves the preparedness and readiness capabilities of the Coast Guard and TSA, while creating a mechanism for port operators to share cyber threat information and best practices.

Chairs of the 9/11 Commission, Tom Kean and Lee Hamilton, have recently called on the Senate to pass this DHS reauthorization. It needs to get to the President's desk and signed into law.

Finally, I'd like to express the committee's appreciation to the leadership and staff of the Port of Los Angeles Harbor Administration for making this event possible.

Chairman MCCAUL. With that, the Chair now recognizes the Ranking Member, Mr. Thompson.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Let me thank you for holding this important hearing on port security today.

I am pleased to be joined by my colleagues here at the Port of Los Angeles in the Congressional district represented so well by Representative Nanette Barragán. As a Member of the committee on Homeland Security, Representative Barragán has been a champion for the Port of Los Angeles and this community. She is a leading voice on matters relating to seaport, port security, and facilitating commerce. We are fortunate to have her as a Member of our committee, and her constituents should be assured she is working hard in Congress on their behalf.

As well as a Dodger fan also.

I want to thank the other Democratic Members for joining us today from nearby Congressional districts. They are Representative Lou Correa, who also is a valued Member of the Committee on

Homeland Security; Representative Norma Torres, a former Member of the committee; and Representative Alan Lowenthal, who represents the neighboring Port of Long Beach.

These Members present here reaffirm their commitment to the security and prosperity of these ports and the surrounding communities. I know they will make this a productive hearing.

Earlier today, we had the opportunity to tour and be briefed about both the Ports of Los Angeles and Long Beach. The scope of the operations by the port and their Federal, State, and local partners is impressive, as is the magnitude of the security challenges facing the ports.

At the same time, the ports are vitally important to trade and commerce, not just locally, but across the country, and around the globe.

Indeed, the bulk of U.S. overseas trade is carried by ships, many of which call on the ports we are discussing today. The economic consequences of a maritime terrorist attack would be catastrophic to the country in addition to the potential loss of life and property.

Unfortunately, port security sometimes gets shortchanged when it comes to allocating scarce Federal security resources. I would argue that rather than spending billions on a border wall, for example, we should invest in better securing our ports by strengthening their physical security, providing appropriate Customs and Border Protection officer staffing, and enhancing cyber defenses.

With respect to staffing, the National Treasury Employees Union, which represent front-line CBP officers at our ports, report that currently nearly 1,500 CBP officer vacancies and an additional 2,000 CBP officers are needed to properly secure our ports while facilitating travel.

This shortage of 3,500 officers is unacceptable. It puts the security of our ports in jeopardy and slows valuable commerce.

Coast Guard resources are similarly strained. For instance, the commandant of the Coast Guard has stated that there were over 500 smuggling events last year about which the Coast Guard had information but unable to respond to due to a lack of assets. Earlier today we heard similar testimony from Coast Guard officials. Again, this is unacceptable.

With respect to cybersecurity, Representatives Barragán and Correa have raised before this committee a major cyber attack that occurred in June of this year at the Port of Los Angeles. A.P. Moller-Maersk had to shut down its container operation, costing the company as much as $300 million, and causing weeks of disrupted operations.

I look forward to hearing from our panel about the lessons learned, the precautions put in place since that incident, and what more remains to be done.

We should be putting our scarce resources toward addressing these gaps in our Nation's security. I hope we can address all of these important issues today and that we can continue to work together to enhance the security of our Nation's port.

In closing, I want to thank the witnesses for joining us today and all the men and women who keep these ports operating securely and efficiently for the benefit of local communities and our entire country.

Again, I appreciate the Chairman convening this meeting and look forward to discussion.

I yield back.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

OCTOBER 30, 2017

Earlier today, we had the opportunity to tour and be briefed about both the Port of Los Angeles and Long Beach. The scope of the operations by the ports and their Federal, State, and local partners is impressive, as is the magnitude of the security challenges facing the ports.

At the same time, the ports are vitally important to trade and commerce not just locally, but across the country and around the globe. Indeed, the bulk of U.S. overseas trade is carried by ships, many of which call on the ports we are discussing today. The economic consequences of a maritime terrorist attack could be catastrophic to the country, in addition to the potential loss of life and property.

Unfortunately, port security sometimes gets short shrift when it comes to allocating scarce Federal security resources. I would argue that rather than spending billions on a border wall, for example, we should invest in better securing our ports by strengthening their physical security, providing appropriate Customs and Border Protection officer staffing, and enhancing cyber defenses.

With respect to staffing, the National Treasury Employees Union (NTEU), which represents front-line CBP officers at our ports, reports there currently nearly 1,500 CBP officer vacancies and an additional 2,000 CBP officers are needed to properly secure our ports while facilitating travel. This shortage of 3,500 officers is unacceptable. It puts the security of our ports in jeopardy and slows valuable commerce.

Coast Guard resources are similarly strained. For instance, the Commandant of the Coast Guard has stated there were over 500 smuggling events last year about which the Coast Guard had information but was unable to respond to due to a lack of assets. Again, this is unacceptable.

With respect to cybersecurity, Reps. Barragán and Correa have raised before the committee a major cyber attack that occurred in June of this year at the port of Los Angeles. AP Moller-Maersk had to shut down its container operations, costing the company as much as $300 million and causing weeks of disrupted operations. I look forward to hearing from our panel about the lessons learned, the precautions put in place since that incident, and what more remains to be done.

We should be putting our scare resources toward addressing these gaps in our Nation's security. I hope we can address all of these important issues today and that we can continue to work together to enhance the security of our Nation's ports.

In closing, I want to thank the witnesses for joining us today and all the men and women who keep these ports operating securely and efficiently for the benefit of local communities and our entire country.

Chairman MCCAUL. Thank you, Ranking Member. I think we have more Members here than some hearings we have in Washington, DC. That says a lot about the Members of the committee and the Members who are locally here in the Los Angeles area. I want to thank you all for being at this hearing.

We are pleased to have a distinguished panel of witnesses before us. First is Admiral Todd Sokalzuk. He is a commander of the Eleventh Coast Guard District for the United States Coast Guard at the Department of Homeland Security.

Next, Mr. Carlos Martel is the director of field operations at the Los Angeles Field Office for U.S. Customs and Border Protection.

We also have Mr. Gene Seroka, and he is the executive director of the Port of Los Angeles.

Mr. Mario Cordero is the executive director of the Port of Long Beach.

Our final witness is Mr. Ray Familathe, the international vice president of the International Longshore and Warehouse Union.

I want to thank all of you for being here today. Your full statements will appear in the record.

The Chair now recognizes the admiral for his testimony.

STATEMENT OF REAR ADMIRAL TODD A. SOKALZUK, COMMANDER, ELEVENTH COAST GUARD DISTRICT, U.S. COAST GUARD, U.S. DEPARTMENT OF HOMELAND SECURITY

Admiral SOKALZUK. Good afternoon, Chairman McCaul, Ranking Member Thompson, and Members of the committee.

I am honored to be here today at the great Port of Los Angeles to discuss the Coast Guard's role in port security.

Mr. Chairman, I would especially thank you. I really want to thank all of you for your leadership and encouraging support of the Coast Guard on this issue.

My complete statement has been provided to the committee and I request to have it entered——

Chairman MCCAUL. Admiral, if you would turn on your microphone.

Admiral SOKALZUK. Just to be clear, I asked that my statement be entered into the official hearing record.

The Coast Guard offers enduring value to our Nation. We are the only branch of the U.S. armed services within the Department of Homeland Security and uniquely positioned to help secure our ports, protect the marine transportation system, and safeguard America's National economic security.

The Coast Guard's governance of the marine transportation system ensures that it remains safe, secure, environmentally sound and productive, particularly with regard to shared critical infrastructure that we rely on for National security, border security, and economic prosperity.

The Coast Guard's efforts to secure our ports and marine transportation system begins far from here, overseas. We leverage international partnerships. Through the International Port Security program, the Coast Guard performs its in-country port security assessments to determine the effectiveness of security and anti-terrorism measures exhibited by foreign trade partners.

We maintain over 40 maritime bilateral law enforcement agreements and 11 bilateral proliferation security initiative ship-boarding agreements. These agreements facilitate international cooperation and allow Coast Guard teams to board and search vessels at sea suspected of carrying illicit shipments, weapons of mass destruction, their delivery systems, or related materials.

The Coast Guard's membership within the intelligence community provides global situational awareness, analysis, and interagency collaboration opportunities with various counterterrorism components, including the Central Intelligence Agency, the National Counterterrorism Center, and the Federal Bureau of Investigation. Intelligence also helps us push our boarders out.

Direct timely intelligence is just a key enabler across a broad spectrum of threats for us. While more than 90 percent of our 2016 at-sea interdictions of illicit narcotics and illegal aliens were cued by intelligence, the Coast Guard's aging major cutters limit our ability to respond to that, even though we have the intelligence.

Critical acquisitions like the off-shore patrol cutter are essential to our long-term success in our fight against transnational criminal organizations.

So while cargo crosses the oceans and nears our shore, Coast Guard personnel co-located with Customs and Border Protection at the National Targeting Center screen ships' crew and passenger information for all vessels required to submit a Notice of Arrival before entering a U.S. port.

As these ships then arrive in American waters, our authorities, through the Maritime Transportation Security Act, provide a robust regime for security plan approval and compliance inspections for both maritime facilities and the vessels.

Area maritime security committees, just like the vibrant one in this area, provide a recurring forum for key agencies and partners to address risk at each port, some of whom you have talked to today.

We support our local partners through our participation in FEMA's port security grant program, and just this year regulated entities within the Los Angeles/Long Beach Port Complex received $11.8 million in Federal grant money to bolster physical and cybersecurity.

In June, we did feel the effects of a cyber event here in this port community. Thankfully, neither of these resulted in marine casualties, but they certainly demonstrated the extents to which cyber vulnerabilities could affect the marine transportation system.

We in the Coast Guard treat cyber as an operational risk, and, to that end, it is part of our enduring competency of managing risk, just like we do across all of our missions.

We continuously work with our partners, continuously work with DHS and across industry to strengthen our relationships to help us to manage this risk and, importantly, with public and private stakeholders.

So for over two centuries, the Coast Guard has safeguarded our Nation's maritime interests, the Coast Guard has layered security strategy, day-to-day operations and coordination across government, to ensure that we are well-positioned to address the broad range of offshore and coastal threats that could impact our National security.

Thank you, Mr. Chairman.

[The prepared statement of Admiral Sokalzuk follows:]

PREPARED STATEMENT OF TODD A. SOKALZUK

OCTOBER 30, 2017

INTRODUCTION

Good morning, Chairman McCaul, Ranking Member Thompson, and distinguished Members of the committee. It is my pleasure to be here today to discuss the Coast Guard's role in port security.

The U.S. Coast Guard is the world's premier, multi-mission, maritime service responsible for the safety, security, and stewardship of the maritime domain. At all times a military service and branch of the U.S. Armed Forces, a Federal law enforcement agency, a regulatory body, a first responder, and a member of the U.S. intelligence community, the Coast Guard operates on all seven continents and throughout the homeland, serving a Nation whose economic prosperity and National security are inextricably linked to broad maritime interests.

America's economic prosperity is reliant on the safe, secure, and efficient flow of cargo through the Marine Transportation System (MTS). The Nation's waterways support $4.5 trillion of economic activity each year, including over 250,000 American jobs.[1] U.S. economic stability, production, and consumption, enabled by the intermodal transportation of goods through the midstream economy, are critical to American prosperity and National security. This trade-driven economic prosperity serves as a wellspring for our power and serves as a leading source of our influence in the world. While we are mindful of the need to facilitate commerce, not impede it, the Coast Guard also recognizes the critical role we play with port partners to reduce risks to U.S. ports and maritime critical infrastructure.

A LAYERED APPROACH

Securing our maritime borders and reducing risk to our ports and infrastructure requires a layered, multi-faceted approach. Because of our unique authorities, capabilities, competencies, and partnerships, the Coast Guard is well-positioned to undertake such an approach and meet a broad range of maritime border security requirements. This layered approach allows the Coast Guard to detect, deter, and counter threats as early and as far from U.S. shores as possible.

For the past 227 years, Coast Guard men and women have patrolled the Nation's ports and waterways to prevent and respond to major threats and hazards. Since Congress established the Steamboat Inspection Service in 1852, Coast Guard prevention authorities have evolved alongside emerging threats and changing port infrastructure. The Coast Guard established Captains of the Port (COTPs) to execute these authorities and work with our partners to prepare our ports for natural disasters, accidents, and deliberate acts. At the same time, as transnational threats to the homeland have increased, so has our reach and overseas presence through foreign engagement and overseas security inspections.

INTERNATIONAL PORT ASSESSMENTS AND VESSEL SCREENING

The Coast Guard conducts foreign port assessments and leverages the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code to assess effectiveness of security and antiterrorism measures in foreign ports. Through the ISPS Program, the Coast Guard performs overseas port assessments to determine the effectiveness of security and antiterrorism measures exhibited by foreign trading partners.

Since the inception of ISPS in 2004, Coast Guard personnel have visited more than 150 countries and approximately 1,200 port facilities. These countries generally receive biennial assessments to verify compliance with the ISPS Code and U.S. maritime security regulations, as appropriate. Vessels arriving in foreign ports that are not compliant with ISPS Code standards are required to take additional security precautions while in those ports. They may also be boarded by the U.S. Coast Guard before being allowed entry to U.S. ports, and in some cases may be refused entry to the United States. In fiscal year 2017, the ISPS Program assessed the effectiveness of anti-terrorism measures in nearly 150 port facilities of 52 of our maritime trading partners, as well as conducted 35 capacity-building activities in 16 countries with marginal port security to prevent them from falling into non-compliance with the ISPS Code.

AREA MARITIME SECURITY COMMITTEES

In U.S. ports, the COTP is designated as the Federal Maritime Security Coordinator (FMSC). In this role, COTPs lead the Nation's 43 Area Maritime Security Committees (AMSCs) and oversee the development, regular review, and annual exercise of their respective Area Maritime Security Plans. AMSCs assist and advise the FMSC in the development, review, and implementation of a coordination and communication framework to identify risks and vulnerabilities in and around ports.

Additionally, AMSCs coordinate resources to prevent, protect against, respond to, and recover from Transportation Security Incidents. AMSCs have developed strong working partnerships between all levels of government and private industry stakeholders. The Coast Guard screens ships, crews, and passengers for all vessels required to submit an Advance Notice of Arrival (ANOA) prior to entering a U.S. port.

[1] "Ports' Value to the U.S. Economy: Exports, Jobs & Economic Growth." American Association of Port Authorities, *http://www.aapa-ports.org/advocating/content.aspx?ItemNumber=21150*, Accessed April 17, 2017.

CYBER RISKS AND THE MARINE TRANSPORTATION SYSTEM

The Coast Guard and the maritime industry continually cooperate to address the risks associated with new threats and technologies. Security threats have evolved from coastal piracy to complex smuggling operations, transnational organized crime, and terrorism. Safety risks have likewise evolved as merchant shipping progressed from sailing ships to ships driven by coal-fired steam boilers, to diesel engines and most recently to liquefied natural gas. Waterfront operations evolved from break bulk cargo to containerization, with sophisticated systems now controlling the movement and tracking of containerized and liquid cargo. The maritime industry is a dynamic industry that includes many components. The maritime industry includes ships and mariners that sail our waters, the ports and facilities they call upon, the waterways upon which commerce moves, and water-borne access to maritime natural resources. Our maritime industry provides vital transportation along marine highways, enables the harvesting of marine and offshore natural resources, supports recreation, and facilitates interstate and international trade. By providing access to transportation, trade, and natural resources, the maritime industry supports our Nation's economic prosperity and is a key driver for our National economy.

The topic of cybersecurity within the maritime industry is as dynamic as any other sector of business. The industry's global reach, large volume of capital transactions, extensive use of commercial services, and reliance on information technology create significant opportunities for exploitation through the cyber domain—the June 2017 notPetya virus and the resulting impacts on APM's global operations, to include subsequent defensive measures, highlighted these risks for the world to see. As evidenced by the notPetya virus, the MTS will continue to experience cyber impacts even though it may not be the intended target. Thus the Coast Guard broadly views cyber as one of many operational risks that must be managed. With the release of the Coast Guard's Cyber Strategy in June 2015, the Coast Guard and their industry partners have engaged in comprehensive efforts to raise maritime cyber risk awareness, enhance preparedness and information sharing, and capitalize on the opportunity to learn from other sectors of the economy. As the Coast Guard transitions from enhancing cyber awareness to promoting improved cyber governance, lessons learned from collaborative efforts led through many of our AMSCs from COTP zones throughout the country, will help inform this important effort.

CONCLUSION

The Coast Guard offers truly unique and enduring value to our Nation. The only branch of our Armed Forces within the U.S. Department of Homeland Security, the Coast Guard is positioned to help secure the border, protect the homeland, and safeguard America's National and economic security. Since 1790, the Coast Guard has helped advance American prosperity by mitigating risk to our Nation's ports and infrastructure to ensure that the MTS operates safely, predictably, and securely. While much has changed from the days of sail, our service has continuously drawn upon our core competencies of mitigating operational risk, and leveraging our crucial partnerships with State, local, Tribal, and industry partners to advance security in U.S. ports.

Chairman MCCAUL. Thank you, Admiral.

The Chair now recognizes Mr. Martel.

STATEMENT OF CARLOS C. MARTEL, DIRECTOR OF FIELD OPERATIONS, LOS ANGELES FIELD OFFICE, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MARTEL. Chairman McCaul, Ranking Member Thompson, esteemed Members of the committee. Thank you for the opportunity to testify today to discuss the role of U.S. Customs and Border Protection in securing maritime cargo, an important responsibility we share with our partners here today.

As lead DHS agency for border security, CBP works closely with our domestic and international partners to protect the Nation from a variety of threats, including those posed in containerized cargo arriving at our seaports.

Serving as the director of field operations for the greater Los Angeles area, including the L.A./Long Beach seaport, the largest seaport in the Nation, I know first-hand how complex cargo security operations are and how valuable our programs and partnerships are to our National security.

CBP has several key programs that enhance our ability to assess cargo for risk, examine high-risk shipments at the earliest possible point, and increase the security of the supply chain. I would like to highlight just a few of these efforts for you today.

First, CBP receives advance information on every maritime cargo shipment, every vessel, and every person before they arrive at the port.

Second, CBP's advanced targeting techniques use the data collected to enhance our ability to assess the risk associated with these cargo shipments and with the entities involved.

Third, our partnerships, those with our DHS and Federal partners, private industry, and foreign counterparts, increase information sharing and enhance our domain awareness, targeting capabilities, and ability to intercept threats at or approaching our seaports.

For example, CBP's Container Security Initiative pushes our security efforts outwards and enables CBP to partner with foreign authorities to identify and examine potentially high-risk maritime containers at the foreign port before they are laden on U.S.-bound vessels.

CBP's 60 CSI ports now prescreen over 80 percent of all maritime containerized cargo imported into the United States.

We also partner with private industry. The Customs Trade Partnership Against Terrorism provides facilitation benefits to rigorously-vetted members of the trade community who volunteer to adopt tighter security measures throughout their entire international supply chain. C–TPAT has grown from 7 initial members to over 11,000 members today.

Finally, advanced, nonintrusive inspection equipment, including X-ray and gamma-ray imaging systems, are placed at domestic and foreign seaports. For example, in partnership with the DHS Domestic Nuclear Detection Office, CBP has deployed nuclear and radiological detection equipment, including radiation portal monitors, radiation isotope identification devices, and personal radiation detectors, to ports of entry Nation-wide.

Radiation portal monitors enable CBP to scan nearly 100 percent of all arriving maritime containerized cargo for the presence of radiological or nuclear materials.

Basically, detection and imaging systems enable CBP officers to examine cargo conveyances, such as sea containers, without physically opening or unloading them. Technology allows CBP to work smarter and faster in detecting contraband and other dangerous materials while facilitating the flow of legitimate cargo.

CBP's detection technology, targeting capabilities, and partnerships are part of a comprehensive strategy that enables CBP to identify and address potential threats in containerized maritime cargo before they arrive at our Nation's seaports.

Thank you for the opportunity to testify today. Be happy to answer any questions.

[The prepared statement of Mr. Martel follows:]

PREPARED STATEMENT OF CARLOS C. MARTEL

OCTOBER 30, 2017

Chairman McCaul, Ranking Member Thompson, and distinguished Members of the committee, it is an honor to appear before you today to discuss the role of U.S. Customs and Border Protection (CBP) in securing maritime cargo. As the lead U.S. Department of Homeland Security (DHS) agency for border security, CBP works closely with our domestic, international, and industry partners to protect the Nation from a variety of dynamic threats, including those posed by containerized cargo arriving at our sea ports of entry (POE).

The United States experiences an immense volume of international trade, a critical component of our Nation's economic security and competitiveness. In fiscal year 2017,[1] CBP officers processed more than 26.1 million imported cargo containers, including 11.9 million maritime cargo containers at our Nation's seaports, equating to $847.7 billion in imports. CBP's cargo security and trade facilitation missions are mutually supportive: By utilizing a risk-based strategy and multi-layered security approach, CBP can focus time and resources on those suspect shipments that are high-risk. This approach incorporates three layered elements to improve supply chain integrity, expedite legitimate trade, promote economic viability, and increase resilience across the entire global supply chain system.

- *Advance Information and Targeting*.—Obtaining information about cargo, vessels, and persons involved early in the shipment process and using advanced targeting techniques to increase domain awareness and assess the risk of all components and factors in the supply chain;
- *Advanced Detection Equipment and Technology*.—Maintaining robust inspection regimes at our POEs, including the use of Non-Intrusive Inspection (NII) equipment and radiation detection technologies; and
- *Government and Private-Sector Collaboration*.—Enhancing our Federal and private-sector partnerships and collaborating with foreign governments to extend enforcement efforts outward to points earlier in the supply chain.

These interrelated elements are part of a comprehensive cargo security strategy that enables CBP to detect, identify, and prevent potential threats, including the use of containerized cargo to transport counterfeit or illicit products, radiological weapons, such as "dirty bombs," or other dangerous materials, before they arrive at our Nation's border. By leveraging intelligence-driven analysis, innovative partnerships, and advanced technology, CBP secures and promotes the movement of legitimate cargo transiting through the maritime environment.

ADVANCE INFORMATION AND TARGETING CAPABILITIES

CBP leverages advance information about cargo, conveyances, and persons, and tailors targeting activities to increase domain awareness and assess the risk of all components and factors in the supply chain. Statutory and regulatory requirements for the submission of advance information, and the development of rigorous targeting capabilities at the National Targeting Center (NTC), enable CBP to identify potential threats and address high-risk shipments before a vessel arrives at a U.S. POE.

The *Trade Act of 2002*,[2] which provides statutory support for the 24-Hour Advance Cargo Manifest rule,[3] also requires importers and carriers to submit to CBP advance electronic cargo information for all in-bound shipments in all modes of transportation. Furthermore, CBP requires the electronic transmission of additional data, as mandated by the *Security and Accountability for Every Port (SAFE Port) Act of 2006*,[4] through the Importer Security Filing and Additional Carrier Requirements rule (also known as "10+2"). These requirements enable CBP to target and mitigate high-risk shipments not just prior to arrival in the United States, but prior to the loading of cargo bound for the United States.

This advance information requirement is a critical element of CBP's targeting efforts at the NTC and enhances CBP's capability to identify high-risk cargo without hindering legitimate trade and commerce. The NTC, established in 2001, coordinates and supports CBP's intelligence and enforcement activities related to the movement of cargo in all modes of transportation—sea, truck, rail, and air. Using

[1] Through August 31, 2017.
[2] Pub. L. No. 107–210.
[3] The 24-hour rule applies only to maritime cargo.
[4] Pub. L. No. 109–347.

the Automated Targeting System (ATS), the NTC proactively analyzes advance cargo information before shipments depart foreign ports. ATS incorporates the latest cargo threat intelligence and National targeting rule sets to generate a uniform review of cargo shipments, and provides comprehensive data for the identification of high-risk shipments. ATS is a critical decision support tool for CBP officers working at the NTC, the Advanced Targeting Units at our POEs, and foreign ports abroad.

ADVANCED DETECTION EQUIPMENT AND TECHNOLOGY

Advanced detection technology is another key aspect of CBP's comprehensive approach to maritime cargo security. NII technology, including X-ray and gamma-ray imaging systems, is placed at domestic and foreign seaports and enables CBP to detect illicit and/or dangerous materials. NII technologies are force multipliers that enable us to screen or examine a larger portion of the stream of commercial traffic while facilitating the flow of legitimate cargo.

CBP currently has 302 large-scale NII systems deployed to, and in between, U.S. POEs. These systems enable CBP officers to examine cargo conveyances such as sea containers, commercial trucks, and rail cars, as well as privately-owned vehicles, for the presence of contraband without physically opening or unloading them. This allows CBP to work smarter and faster in detecting contraband and other dangerous materials. As of September 1, 2017, CBP has used the deployed NII systems to conduct more than 86 million examinations, resulting in more than 20,600 narcotics seizures.

Scanning all arriving conveyances and containers with radiation detection equipment prior to release from the POE is an integral part of the CBP comprehensive strategy to combat nuclear and radiological terrorism. In partnership with the Domestic Nuclear Detection Office (DNDO), CBP has deployed nuclear and radiological detection equipment, including 1,280 Radiation Portal Monitors (RPM), 3,319 Radiation Isotope Identification Devices (RIID), and 35,294 Personal Radiation Detectors (PRD) to all 328 POEs Nation-wide.[5] Utilizing RPMs, CBP is able to scan 100 percent of all mail and express consignment mail and parcels; 100 percent of all truck cargo, 100 percent of personally-owned vehicles arriving from Canada and Mexico; and nearly 100 percent of all arriving sea-borne containerized cargo for the presence of radiological or nuclear materials. Since the inception of the RPM program in 2002 through August 2017, CBP has scanned more than 1.4 billion conveyances for radiological contraband, resulting in more than 6.1 million alarms in primary and secondary operations, all of which have been successfully adjudicated at the proper level.

CBP continues to look for more capable technologies that are more efficient and effective. For example, a key enabler of RPM efficiencies in the maritime environment is employing the concept of remotely-operated RPM lanes at select seaports. CBP, together with DNDO, worked on a pilot throughout fiscal year 2017 to pilot RPM remote operations at the seaport in Savannah, Georgia. The goal is to provide CBP field offices and ports with increased flexibility to reduce RPM operations staffing demands and redirect staff to other high-priority mission areas where and when feasible.

In conjunction with CBP's targeting capabilities, advancements in cargo screening technology provide CBP with a significant capacity to detect illicit nuclear and radiological materials and other contraband, and continue to be a cornerstone of CBP's multi-layered cargo security strategy.

GOVERNMENT AND PRIVATE-SECTOR COLLABORATION

A critical and complementary component of CBP's effort to expand and strengthen cargo security is our extensive domestic and international partnerships with private industry and Government counterparts. Close collaboration with our partners increases information sharing, which, in turn, enhances CBP's domain awareness, targeting capabilities, and ability to intercept threats at, or approaching, our borders.

Federal Government Partnerships

CBP works closely with its DHS partners, including the U.S. Coast Guard (USCG), U.S. Immigration and Customs Enforcement (ICE), and the Science and Technology Directorate (S&T) to coordinate cargo security operations and deploy advanced detection technology. Since 2011, CBP, USCG, and ICE have coordinated security activities through the cross-component Maritime Operations Coordination (MOC) plan. The plan addresses the unique nature of the maritime environment and sets forth a layered, DHS-wide approach to homeland security issues within the

[5] As of September 1, 2017.

maritime domain, ensuring integrated planning, information sharing, and increased response capability in each area of responsibility. CBP also collaborates with DNDO as well as with numerous agencies within the U.S. Departments of Defense, Energy, Health and Human Services, Commerce, Justice, and Treasury to promote real-time information sharing.

CBP has participated in numerous joint-operations with government partners that led to the interdiction of illicit shipments. For example, Project Zero Latitude was developed due to escalation of foreign and domestic narcotics interceptions involving sea containers of produce and seafood shipments, particularly involving Ecuador. At the NTC, CBP conducted an analysis of historical ATS information and cocaine seizure data. The analysis enabled NTC to identify several smuggling trends that will facilitate the identification of future suspect shipments.

International Partnerships

CBP also extends its cargo security efforts outward through strategic partnerships with foreign countries through the development of international cargo security programs and initiatives. One of CBP's most effective international cargo security programs is the Container Security Initiative (CSI). This initiative was established in 2002 with the sole purpose of preventing the use of maritime containerized cargo to transport a weapon of mass effect/weapon of mass destruction by ensuring all containers identified as potential risks for terrorism are inspected at foreign ports before they are placed on vessels destined for the United States. Through CSI, CBP officers stationed at CSI ports abroad and the NTC in Virginia work with host countries' customs administrations to identify and mitigate containers that may pose a potential risk for terrorism based on advance information and strategic intelligence. Those administrations use a variety of means, including detailed data assessment, NII, radiation detection technology, and/or physical examinations to screen the identified high-risk containers before they depart the foreign port.

CBP works closely with CSI host country counterparts to build their capacity and capability to target and inspect high-risk cargo. Today, in addition to weapons detection, many CSI ports are now also targeting other illicit materials, including narcotics, pre-cursor chemicals, dual-use technology, stolen vehicles, weapons and ammunition, and counterfeit products. Furthermore, advancements in technology have enabled CBP to increase the efficiency of CSI operations without diminishing effectiveness by conducting more targeting remotely at the NTC. CBP's 60 CSI ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America currently prescreen over 80 percent of all maritime containerized cargo that is imported into the United States.

CBP's strong working relationship with our foreign partners is also exemplified by the Secure Freight Initiative (SFI) in Qasim, Pakistan. Through SFI-Qasim, 100 percent of containerized maritime cargo is scanned (by both radiation detection and imaging equipment) prior to lading on-board a U.S.-bound vessel. All targeting of containers and monitoring of the scanning is done remotely via live video feed by CBP officers working at the NTC. Physical examinations are conducted at Port Qasim by Pakistani Customs officials and locally-engaged staff hired and vetted by the U.S. Consulate General in Karachi. These physical examinations are also monitored by live-feed at the NTC.

Creating the process for real-time data transmission and analysis in Qasim required the development, installation, and integration of new software and equipment. CBP partnered with the U.S. Department of Energy (DOE) to deploy networks of radiation detection and imaging equipment in Qasim. Port Qasim continues to showcase the SFI program in a country where the government and terminal operators support the initiative, and where construction of dedicated facilities is possible. From constructing the scanning site to providing adequate staffing levels for SFI, the government of Pakistan remains a strong partner in deploying SFI operations.

In addition to Port Qasim, Pakistan, since March 2014, CBP also scans 100 percent of all U.S.-bound cargo containers from the Port of Aqaba, Jordan, using trained and vetted foreign-service nationals to transmit scan data in real-time to the NTC. Similar to implementing operations in Qasim, CBP received the full support of the Government of Jordan to implement 100 percent scanning in Aqaba. In addition to that support, successful implementation of 100 percent scanning was possible due to the low-to-medium volume of U.S.-bound cargo processed through the port, and the small percentage of transshipped cargo, which allowed scanning equipment to be placed at the entrance to the port so as not to hinder the flow of cargo movement.

The impact of these programs has been amplified by the close collaboration between CBP and DOE's Office of Nuclear Smuggling Detection and Deterrence

(NSDD). Many CSI ports integrate into their operations partner country radiation detection equipment deployed by NSDD. In a similar fashion, CBP and NSDD collaborated in the detection equipment installation at the SFI operations in Qasim. The strong coordination between CBP and NSDD extends to information and resource sharing that enhances the security of maritime supply chain.

All trading nations depend on containerized shipping for the transportation of manufactured goods, which underscores the importance of international programs such as CSI and SFI. Collaboration with foreign counterparts provides increased information sharing and enforcement, further secures the global supply chain, and extends our security efforts outward.

Private-Sector Partnerships

An essential component of CBP's cargo security operations is our close and effective collaboration with private industry partners. For example, CBP works with the trade community through the Customs Trade Partnership Against Terrorism (CTPAT) program, which is a public-private partnership program wherein members of the trade community volunteer to adopt tighter security measures throughout their international supply chains in exchange for enhanced trade facilitation, such as expedited processing. CTPAT membership has rigorous security criteria and requires extensive vetting and on-site visits of domestic and foreign facilities. This program has enabled CBP to leverage private-sector resources to enhance supply chain security and integrity.

CTPAT membership has grown from just 7 companies in 2001 to more than 11,180 certified partners today, accounting for more than 54 percent (by value) of goods imported into the United States. The CTPAT program continues to expand and evolve as CBP works with foreign partners to establish bi-lateral mutual recognition of respective CTPAT-like programs. Mutual Recognition as a concept is reflected in the World Customs Organization's Framework of Standards to Secure and Facilitate Global Trade, a strategy designed with the support of the United States, which enables customs administrations to work together to improve their capabilities to detect high-risk consignments and expedite the movement of legitimate cargo. These arrangements create a unified and sustainable security posture that can assist in securing and facilitating global cargo trade while promoting end-to-end supply chain security. CBP currently has signed Mutual Recognition Arrangements with New Zealand, the European Union, South Korea, Japan, Jordan, Canada, Taiwan, Israel, Mexico, Singapore, and the Dominican Republic and is continuing to work toward similar recognition with China, Brazil, Peru, Uruguay, and India.

CBP also collaborates with port and terminal operators to enhance its agility, responsiveness, operational efficiencies, and unwavering commitment to our mutually supporting objectives of safety, security, and prosperity. CBP recently launched the Advanced Qualified Unlading Approval Lane (AQUA Lane), an expedited clearance system for CTPAT sea carriers arriving at CTPAT terminal port operators that qualify under a set of predetermined mandates to allow them to immediately unlade their cargo (only) upon arrival in the United States. This CTPAT benefit provides the trade community with monetary savings in terms of labor costs, as well as additional container movement efficiency and delivery predictability.

CBP has also been re-engineering our operations in collaboration with the Port of Los Angeles' Trans Pacific Container Service Corporation (TraPac). The TraPac terminal in the Port of Los Angeles has invested in technology and infrastructure to upgrade the terminal to an automated terminal environment that supports both the targeted NII X-ray/gamma-ray imaging of targeted commerce, and the 100 percent mandated radiation scanning of all incoming commodities at the TraPac terminal. In a joint effort, TraPac, DNDO, and CBP developed a new and innovative method for automated radiation scanning of in-bound containers in the terminal's intermodal rail yard. Since December 2016, the terminal's automated conveyor systems transport in-bound containers through CBP RPMs before the containers are loaded onto railcars.

Similar to TraPac, through a public-private partnership agreement, CBP and DNDO continue to work with the Northwest Seaport Alliance to employ a straddle carrier portal at the Pierce County Terminal in Tacoma, Washington. The straddle carrier portal will provide a fixed portal radiation scanning capability that will require fewer CBP personnel to conduct radiation scanning of cargo containers and will allow the port to regain some of its operational footprint and more quickly process cargo destined for rail transportation.

CONCLUSION

CBP's targeting activities and advanced technology enhances CBP's capability to assess whether U.S.-bound maritime cargo poses a risk to the American people.

Working with our government, international, and private industry partners, CBP's cargo security programs help to safeguard the Nation's borders and our seaports from threats—including those posed by radiological weapons.

Chairman McCaul, Ranking Member Thompson, and distinguished Members of the committee, thank you for the opportunity to testify today. I would be pleased to answer your questions.

Chairman MCCAUL. Thank you, Mr. Martel.

Chair now recognizes Mr. Seroka.

STATEMENT OF EUGENE D. SEROKA, EXECUTIVE DIRECTOR, THE PORT OF LOS ANGELES

Mr. SEROKA. Thank you, Chairman McCaul, Ranking Member Thompson, and Members of the House Homeland Security Committee.

My name is Gene Seroka. I am the executive director here at the Port of Los Angeles. On behalf of our mayor, Board of Harbor Commissioners, along with the women and men who do the work at our port complex, it is a distinct honor to host this important and timely hearing at America's port.

Today's hearing seeks to examine the physical and cybersecurity of our Nation's ports. I cannot think of a better place to begin that examination than right here at the Port of Los Angeles.

While the port is immense in scale, covering 7,500 acres of land, 43 miles of waterway, 100 miles of rail configuration, including 27 terminals and 270 berths, its scale is perhaps exceeded only by its scope.

We are the Nation's busiest container port. Setting a record among last year as the busiest container port in the Western Hemisphere, moving more than 9.2 million 20-foot equivalent units.

Together with our neighboring Port of Long Beach, we handle goods to and from each and every one of our Nation's 435 Congressional districts, account for more than 40 percent of our Nation's imports, and 30 percent of our Nation's exports.

All told, the trade through our complex has an economic impact in excess of US$311 billion and related to over 3 million jobs throughout the country.

The scale and scope of our cargo operations gives us an outsized role in the Nation's economic prosperity. So it is a matter of course that we treat our responsibility to protect this critical piece of America's trade infrastructure with the highest of importance.

Security starts with our Los Angeles Port Police force, a specialized law enforcement agency that operates 24 hours a day, 7 days a week, protecting the port from threats, whether it be by land, sea, air, or cyber space.

The capabilities of our police force include canine units used to search vessels and containers, full-time dive unit to inspect critical infrastructure, and sea marshals program for all inbound and outbound cruise ships and vessels of interest.

Our Port Police has a long and impressive track record of successful joint operations with other law enforcement agencies, our State partners and Federal partners alike, including the United States Coast Guard, the FBI, Secret Service, Department of Homeland Security, and especially Customs and Border Protection.

There are two areas the Federal Government can assist our Port Police in maintaining the physical security of the port complex: Training and equipment.

With respect to training, the Port Police provides only POST-Certified and Federally-recognized regional Maritime Law Enforcement Training Center on the West Coast of the United States. We call it MLETC.

The curriculum, approved by Federal Law Enforcement Training Center, includes coursework in law enforcement, maritime operations, underwater improvised explosion detection, tactical and boarding operations training. The MLETC also hosts Federally-recognized emergency management training, as provided by Texas A&M engineering extension.

Future grant funding or Federal support would help us enormously in this continuing effort to provide a highly specialized training right here on the West Coast.

With respect to equipment. The extended border efforts of CBP, internationally and Nationally, is of great importance to the region and the Nation.

We ask for support in CBP's recapitalization projects to leverage technology and human effort in the detection of weapons, contraband, and emerging highly dangerous narcotics, as demonstrated by the deadly opiate epidemic.

As you know, many of these substances are incredibly toxic, deadly to users, and of great concern to unsuspecting labor, workers, law enforcement personnel, among others, that encounter these compounds.

Finally, I would like to focus my remaining remarks on cybersecurity. The Port of Los Angeles is especially sensitive to the needs for cybersecurity protection because of our organization and the rest of the maritime shipping industry, for that matter. It is becoming increasingly reliant on digital industrial infrastructure.

In 2014, the port established the Nation's first port cybersecurity operations center. Some of you witnessed that today, where more than 20 million cyber intrusion attempts per month are thwarted right here at the Port of Los Angeles. That is 7 to 8 attacks every second on our port complex.

The center is run by a dedicated cybersecurity team and acts as a centralized location proactively monitoring network traffic to prevent and defect cyber incidents. It is also able to contain and manage any attacks that can be discussed with law enforcement agencies, like the FBI, the Secret Service, and local law enforcement for investigation purposes.

But we know there is much more that needs to be done. The recent cyber attack on Maersk and A.P. Moller terminals was a call to action for all of us. We know that we must move swiftly to address cross-sector risk.

The port ecosystem is a complicated one, relying on vendors, logistics companies, multitudes of clients, and transportation service providers. Adding in other critical infrastructure providers like energy, communications, information technology sectors, and the need to address our collective vulnerability becomes an absolute necessity for all.

To that end, we recommend continued and focused engagement with the broader maritime industry to identify and disseminate best practices, assist in assigning roles and responsibilities, assist in educating, informing, and improving the way industry conducts vulnerability assessments, leverage port security grant programs to incent cybersecurity applications, and look at ways to improve information sharing in and across the maritime industry, promoting cybersecurity awareness, preparedness, and response standards.

With that, I conclude my remarks for this afternoon.

[The prepared statement of Mr. Seroka follows:]

PREPARED STATEMENT OF EUGENE D. SEROKA

OCTOBER 30, 2017

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 industry's largest companies, Maersk, was compromised by a cyber attack. The global cybersecurity attack called "nonPetya" 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 legisla-

tion 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 7 to 8 attacks every second on average. The Port is seeing a growing volume and variety of malicious cyber attacks 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 cybersecurity 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 Nation-wide 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 21st Century.

Chairman MCCAUL. Thank you, Mr. Seroka.

The Chair now recognizes Mr. Cordero.

STATEMENT OF MARIO CORDERO, EXECUTIVE DIRECTOR, THE PORT OF LONG BEACH

Mr. CORDERO. Thank you, Chairman.

Chairman McCaul, Ranking Member Thompson, and Members of the committee, thank you for the opportunity to speak on port security matters this afternoon.

My name is Marco Cordero, and I am the executive director of the Port of Long Beach. Prior to joining the port, I served as chairman of the Federal Maritime Commission. As a former Federal appointee, I can appreciate the importance of Federal and local partnership with regard to securing our Nation's ports.

As the second-busiest seaport in the United States, the Port of Long Beach is a major gateway for U.S.-Asia trade. We support more than 1.4 million jobs Nation-wide, and in 2016 moved more than 6.8 million TEUs, also known as containers. We are on pace for 7 percent growth for year-end 2017.

Combined with the Port of Los Angeles, we comprise the busiest port complex in the Nation and the ninth busiest in the world. In 2016, combined, we moved 400 billion in containerized trade, which is 40 percent of the Nation's import cargo.

Since the terror attacks of September 2001, the port has received more than 1.6 billion in Federal grants to compliment the extensive investments by the port, the city of Long Beach, marine terminal operators, and carriers to ensure that the Nation's largest container gateway remains open and safe.

This is a multi-layer security effort that requires the continued participation of funding by our Federal partners. We appreciate the Federal support and hope that this program will not be further reduced beyond the annual $100 million appropriation.

The safety and security of the port is of utmost importance. Our Joint Command and Control Center, a 24/7 maritime domain

awareness center, is a critical hub for coordinating security efforts that include partnerships with local, State, and Federal law enforcement agencies as well as maritime and private-sector stakeholders.

Through innovative efforts, the port has a monitoring network of over 400 cameras, a comprehensive fiber-optic network, an integrated security management system for synchronized monitoring, and quick threats detection, access control and alarm monitoring, boat patrols, radar systems, a vessel tracking system, and sonar equipment.

Securing the flow of goods to and from the United States is a complex mission involving numerous partners across the globe. Together, 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.

We understand the Congressional interest in 100 percent scanning of all incoming cargo. Although a worthy goal, there are formidable practical challenges for ports like Long Beach and Los Angeles that handle over 15 million containers per year. Such challenges include technology and funding for equipment and personnel to handle these high volumes.

We see value in deepening the level of engagement with global partners and utilizing big data to target those containers that pose a concern.

The port also strongly supports the continuation of programs like the Customs Trade Partnership Against Terrorism that incentivized shippers to secure each step in the supply chain.

Landside security is of critical importance. The port is extending additional layers of protection by developing analytics and sensors to better forecast the landside movement of goods to and from the port, rely heavily on information technology to operate as well as to secure the port and complex and its assets.

As you know, with increased reliance on technology comes the increase on ability to cyber attack. As an example, the port's information management division successfully thwarts over 30 million threats a month.

In addition to man-made cyber threats, the maritime sector is also susceptible, as we all know, to technology disruption from natural hazards and disasters.

Business resiliency is a critical part of the port's on-going cybersecurity planning. Preparation, response, and recovery planning are paramount to ensure that we assume operations swiftly. 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.

There is not a one-size-fit-all solution because each port has a different business model. Our information management division has developed and implemented an enterprise-wide on-line cybersecurity awareness training program. It is believed that once cyber operations are understood on an enterprise-level systems and protocols can be organized to continuously promote cybersecurity throughout the organization.

We also understand the importance of vulnerability assessments to identify the prioritized gaps that could lead to interruptions affecting key operations. The port has undergone regular assessments over the years and plans to continue this practice.

Our decisions must be information-driven. An environment that promotes the sharing of information which includes balancing the need to protect property information, or proprietary information, with protecting our National critical infrastructures.

Last, a new and potential threat to safety and security is that of unmanned aerial systems.

The unhindered operation of UAS near terminals and ships could pose an immediate danger to the port complex and operations. UAS operations in vulnerable areas must be restricted and local first responders should be deemed the enforcement entity authorized to mitigate threats. We believe this type of enforcement is better delegated to local public safety personnel working in conjunction with Federal partners.

Mr. Chairman, thank you for the opportunity to address the committee. Protecting U.S. ports must be a core capability of our Nation. We appreciate the support of this committee, and we stand ready to work with you and your staff to protect the people and economic vitality of our ports.

[The prepared statement of Mr. Cordero follows:]

PREPARED STATEMENT OF MARIO CORDERO

OCTOBER 30, 2017

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, cybersecurity 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 20-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 multi-layered 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.

Cybersecurity

Information Technology Risk and Cybersecurity

The number of U.S. data breaches across educational institutions, shipping firms, Government agencies, military, medical facilities, financial firms and other busi-

nesses 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, cybersecurity 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 man-made 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 on-going cybersecurity 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 cybersecurity, 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 cybersecurity 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 on-going 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 on-line cybersecurity 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 cybersecurity 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 cybersecurity 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 cybersecurity throughout the organization. Legacy systems can be evaluated and updated to meet the ever-changing cybersecurity 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 cybersecurity 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 committee and we are active participants and the Information Technology function provided a presentation on the latest information on proactively preventing cyber attacks. This information was shared with everyone and provided to the USCG leader for inclusion in the on-going sharing efforts. In 2016, the Port of Long Beach staff participated in Cyber Guard 2016, a National-level cybersecurity 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 cybersecurity 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 cybersecurity posture. There should not be one-size-fits-all approach to managing cybersecurity 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 pre-emption, 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 cybersecurity or fragmented tactical-level technical detail. Focusing on the development of common frameworks and strategic policies is sorely needed. A road map that provides guidance and flexibility for industry decisions makes sense and will strengthen our National cybersecurity 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.

Chairman MCCAUL. Thank you, sir.

Chair now recognizes Mr. Familathe.

STATEMENT OF RAY FAMILATHE, INTERNATIONAL VICE PRESIDENT, INTERNATIONAL LONGSHORE AND WAREHOUSE UNION

Mr. FAMILATHE. Good afternoon, Chairman McCaul and Members of the committee.

Thank you for inviting me here to speak on the security of America's ports. I am here on behalf of the 50,000 members of the International Longshore and Warehouse Union, ILWU, working at America's West Coast, Alaskan, and Hawaiian ports.

The men and women of the ILWU are not only the first put at risk by a terrorist attack on a port, they are also a vital part of our first line of defense.

During any emergency at a port, our members work hand-in-hand with emergency responders to do everything from containing fires and chemical releases to moving endangered or dangerous cargos.

Our skills and knowledge of the waterfront are invaluable. Among our ILW members are the Los Angeles Port Police, a model 125-officer dedicated work force to port safety and security.

Following a port emergency, it is our members who work rapidly to recover port operations. That is why port security is so important to us and why we want to see the American taxpayer get the most benefit for all the dollars they invest in Federal port programs.

It is our view that the Transportation Worker Identity Credential program, TWIC, is a costly failure. Roughly 750,000 American maritime workers are covered by TWIC. It costs between $300 to $500

per person just to apply for and renew the credentials over a 10-year period. That is roughly $225–375 million just in TWIC application costs to our industry.

TWIC readers are also expensive. As the GAO reported in 2012, readers are often unreliable. The new Coast Guard rules in 2016 on TWIC readers at the passenger facilities will alone cost the industry another $157.9 million over 10 years.

The Federal Government itself spends tens of millions more on staffing the TWIC program, processing applications, and spot-checking credentials. It also provides millions more in port security grants tied to the TWIC program.

Yet, despite spending of hundreds of millions of dollars on TWIC, no attacks have been identified as having been stopped by TWIC. No experts cite TWIC as an impediment to future terrorist attacks on American ports.

TWIC does produce one result: Hardship for waterfront workers. Despite the law saying TWIC applications will be processed in less than 30 days, TSA reports that TWIC enrollment delays are more than 60 days.

More than 50,000 workers have had to file appeals after an initial TWIC denial. On an appeal, the burden is on the worker to prove that he or she is, in fact, eligible for TWIC. Due to the large volumes of processing, TWIC appeals can take up to 6 months. During all of these delays, the worker cannot even get unemployment insurance.

Money from TWIC could better be invested in many beneficial programs, including budgeting for an increase in CBP officers on the front lines at the ports of entry. Not only does a stronger inspection force improve security, it makes ports more efficient. Our ports cannot offer extended hours or weekend shifts to reduce freight congestion if CBP lacks officers.

We also question the need for more spending on cameras. The Port of Los Angeles alone has 700 cameras linked to its security center, and other ports are equally saturated.

Would it not be wise to invest our money in closing the real gaps in security?

The ILW believes the threat from cyber attacks is such a gap. This includes hacks to TWIC data systems.

TWIC data can reveal not only personal information, but it shows the work patterns of thousands of water-front workers. That is high-value information to anyone planning a terrorist attack on a port.

In June 2015, Maersk, the world's largest shipping line, was attacked by an unknown actor with a variation of a ransomware attack. This attack affected 17 Maersk terminals world-wide, including along America's West Coast where the ILW works. Maersk estimated damages between $2- and $300 million.

The Maersk terminal in Los Angeles, the port's largest terminal, was closed for days. Delays continued to ripple through Maersk's system globally for weeks. Operations at Maersk terminals in Los Angeles and the Pacific Northwest returned to work only because ILW members still had the know-how how to temporarily return to paper-based operations.

Imagine the damage to our National security if port operations were brought to a standstill at just the time America is moving critical military equipment and supplies to respond to an international crisis or when our armed forces are already in combat.

We would be fools not to assume that America's opponents, who have already launched major cyber attacks on U.S. computer systems, have not also considered this scenario.

The ILW believes this is the time to review our port cybersecurity. We believe this is the time to review the critical dollars we are investing in port security, physical and cyber, to assure we are providing our country with the best protection.

The ILWU representing the men and women who have built their careers working on the waterfront thank each of you for your commitment to our ports, and we promise you will have our full support in genuinely improving port security.

That concludes my remarks.

[The prepared statement of Mr. Familathe follows:]

PREPARED STATEMENT OF RAY FAMILATHE

OCTOBER 30, 2017

Good afternoon Chairman McCaul and Members of the committee: Thank you for inviting me to testify on the state of the physical and cybersecurity at our Nation's ports. I am here today on behalf of the approximately 50,000 members of the International Longshore and Warehouse Union (ILWU). The ILWU represents longshore, warehouse, and maritime workers in the States of California, Washington, Oregon, Alaska, and Hawaii.

As a union, we have actively worked to improve port safety and to reduce the risk of terrorism at our work sites. Our members are not only among the first men and women that would be put at risk by a terrorist attack on an American port, they are also a vital component of our country's first line of defense. Our highly-skilled workers are critical to any emergency response within a West Coast port, whether it is operating cranes and heavy equipment to move vulnerable or dangerous cargo from harm's way, or contributing our know-how to containing fires and limiting release of harmful commodities. Longshore workers are in fact natural allies of law enforcement and first responders on the waterfront.

Indeed, our members include the Los Angeles Port Police, a model 125-officer force dedicated to port safety and security. This specialized police force has over 100 years of experience protecting our ports, and hosts a joint terrorism squad tasked with preventing attacks on our maritime facilities.

ILWU members also serve on the maritime security committees operated by our ports, and we strongly encourage our port industry partners to fully integrate the union into their command and control centers, including union participation in planning and emergency response drills. As a partner in port security, we not only help guard against and respond to acts of terror, but also our members are critical to assuring a rapid recovery of port operations.

Without a doubt, the ILWU takes port safety and security seriously and we strongly support programs that genuinely contribute to protecting our members and America's ports. Unfortunately, not all Federal programs meet that standard. I would like to address one program that has demonstrated no effect on better securing our ports—the TWIC program. The reality is that in a modern container facility, the longshore worker has no real access to the cargo, and the documentation associated with a container's contents is not available to the worker. TWIC credentialing of longshore workers is, as a practical matter, a feel-good measure promoted by those who do not understand modern container terminal operations as a way to appear to being addressing public and political concern about port security. The reality is that TWIC does nothing to mitigate the real threat—container access outside the terminal throughout the supply/transportation chain.

TWIC is also an expensive program for workers, our employers and for the Federal taxpayer. An estimated 750,000 American maritime workers are covered by TWIC, at an approximate cost of $300 to $500 per person to apply for the needed credentials and renewals over 10 years. That is roughly $225 to $375 million dollars just in TWIC application costs to the industry. Just the recently-issued Coast Guard

rules on TWIC readers at passenger facilities alone is estimated to cost industry another $157.9 million over 10 years. In addition, the Federal Government spends tens of millions of dollars on staffing the TWIC program, processing applications, and spot-checking credentials. It has also provided millions more in port security grants to port authorities tied to the TWIC program. Yet despite the expenditure of hundreds of millions dollars on TWIC—making TWIC the maritime industry's most costly security program, eating up an enormous percentage of our limited funds for port security—no one can point to any genuine gain in the fight against terrorism. No attacks have been identified as having been deterred by TWIC. No experts cite TWIC as an impediment to potential terrorist attacks on American ports. TWIC is simply a costly failure for the industry and for the American taxpayer.

Furthermore, we are not convinced that TWIC readers will work in a maritime environment. A GAO report on the TWIC pilot program released in February 2012 concluded that "readers capable of passing all environmental tests would represent a serious business challenge to manufacture in terms of cost per unit." Further, a high number of cards malfunctioned electronically. Durability of the card is a serious issue. Sun, wind, grime, dust on cards caused fading, stained and peeling cards that have difficulty being read by TWIC readers. Further, participants in the pilot program said they would reduce the number of guards when the reader was installed—the same guards who know the names and faces of the regular workforce.

As well as being a failed security program, TWIC is a significant hardship on those 750,000 Americans who work on the waterfront. Not only is it expensive to apply for the TWIC credentials, but also the application process itself is rife with bureaucratic delays and hardships. As recently as February 2015, the TSA reported TWIC enrollment delays of more than 60 days and recommended that applicants apply for their TWICs at least 10 to 12 weeks early. Those delays occurred despite a statutory requirement to respond to the applicant within 30 days. In addition to major delays, applicants face the need for two or more in-person meetings at the nearest TWIC office just to apply and later collect the credentials.

During consideration of port security legislation, the ILWU has advocated for a background check limited to "terrorism security risks," and to ensure that there is due process for workers denied a TWIC card. However, we remain concerned that in a number of instances, TWIC has been used to single out workers who may have an old felony charge in their background but do not pose a terrorism security risk.

Further, since implementation of the TWIC program, more than 50,000 workers filed for appeals after an initial TSA determination that the worker was ineligible to receive a TWIC. On an appeal, the burden is on the worker to prove that he or she was not convicted of any felony by obtaining court and police records and sending them to the TSA. TSA issues interim denials in all cases when the record on file with the FBI is an open arrest for a disqualifying offense. Even if the arrest has been dismissed by local law enforcement, local officials often fail to update this status with the FBI. In short, the FBI database is far from complete, yet TSA relies on it exclusively. Due to the large volumes, the processing of TWIC appeals and waivers at one time took over 6 months, during which time the worker cannot work or even obtain unemployment insurance.

At a minimum, the ILWU strongly urges this committee to draft legislation to place the onus on TSA—not the worker—to obtain court and police records when the FBI database is incomplete. It is a considerable hardship that workers must prove they have no disqualifying convictions before obtaining a TWIC card.

Recognizing the inadequacies of this very same FBI datebase, Congress puts the burden on the FBI to fill the missing gaps when it conducts background checks for gun purchases. Why should American workers be treated more harshly when it is their very livelihoods at stake?

Another issue that should be of concern to Members of this committee, is container access outside the terminal throughout the supply/transportation chain. Prior to 9/11, ILWU marine clerks were assigned responsibility to ensure that seals on containers were not tampered with before entering the port complex, and ensuring that unsealed empty containers were not carrying contraband or even people. Cameras have replaced people to perform this function, but cameras cannot verify that seals have not been broken and resealed. Only by yanking on the seal and inspecting its integrity with human eyes can we determine if the seal has been tampered with en route. Cameras also cannot see a hidden compartment inside an empty container. We stand ready to assist in this effort if the Coast Guard decides it is a necessary component of port security.

In addition to recognizing the role humans play in inspecting containers, Customs and Border Protection (CBP) staffing is also critical to safe and efficient port operations. Given the enormous responsibilities of CBP—in scale and importance—Congress needs to provide a budget that puts a full roster of CBP officers on the front

lines at our ports of entry. Not only are CBP officers the lead force for inspecting goods and passengers when entering the United States, but at America's ports our work comes to a stop without adequate CBP staffing. Our ports cannot offer extended hours or weekend shifts to reduce freight congestion if CBP lacks officers. These officers are key to getting imports and exports efficiently and safely moving through America's ports.

The ILWU also recognizes the multiple threats presented by cyber attacks. This includes potential hacks into public and private systems that collect TWIC data. TWIC data can reveal not only personal information, raising the risk of identity theft, but it also reveals the work patterns of thousands of waterfront employees. That is information of high value to anyone planning a terrorist attack or criminal activity at a port. It is now far easier for hostile interests to simply employ the skills of any of the tens of thousands of individuals and criminal organizations around the world with expertise in cyber attacks than it is to invest years in trying to recruit and radicalize a random waterfront worker who only has limited access to data and cargo. We need to take port cybersecurity seriously and stop using ineffective measures like TWIC.

We would also be foolish not to acknowledge that we are at risk from cyber attacks not just from terrorist organizations, but from hostile governments in Russia, Asia, and elsewhere. In an era where wars are now often preceded or replaced by cyber attacks, ports are vulnerable. And bad actors have already shown what they can do with a cyber attack on maritime facilities.

On June 29, 2017, the *Los Angeles Times* carried this headline, "Maersk's L.A. port terminal remains closed after global cyber attack." Maersk, the world's largest shipping line was attacked in June by unknown actors with a variation on a ransomware attack called "NotPetya." This attack affected at least 17 Maersk terminals world-wide, including several along America's West Coast where the ILWU works. Maersk estimated its damages at between $200 to $300 million dollars. The Maersk terminal here in Los Angeles, the Port of Los Angeles' largest terminal in fact, was closed for days. Delays continued to ripple through Maersk's system for weeks after the attack. Operations at Maersk terminals in the Pacific Northwest return to work only because ILWU members had the know-how to temporarily return the terminal to paper-based operations.

This attack, which impacted other companies as diverse as FedEx and drug manufacturer Merck, was actually designed to destroy data files and cripple operations—not hold computer systems hostage for ransom payments. The maritime industry is considered at high risk from such attacks due to the wide-spread use of older technology. This attack was so sophisticated however that it badly impacted Maersk, the company considered our industry's technology leader. If this attack had hit other major freight companies that lack Maersk's more advanced technology, the damage to port and maritime operations could have been far worse. Imagine the damage not just to our economy but to our National security if major port operations on the West Coast were brought to standstill for days at just the time America is moving critical military equipment and supplies to respond to an international crisis or when our armed forces are already in combat. We would be negligent and foolish to not assume that America's opponents—who have already launched major cyber attacks on our private and public computer systems—have not also considered this scenario.

The ILWU believes the time to comprehensively review our port cybersecurity is now. We believe it is time to review the critical dollars we are investing in port security—physical and cyber—to assure we are providing America the best protection.

Port security grants should be awarded based on their real impact on security, with an increasing priority on funding cybersecurity. We have enough cameras on the docks, many of which are used to monitor worker performance rather than monitoring for illegal entry. In fact, we already have over 700 cameras that are tied into the threat detection center just here at the Port of Los Angeles.

We also have enough fences paid for by U.S. taxpayers. The Port of Stockton actually used a port security grant to place a fence in a seemingly illogical narrow space at its river port. Ironically, this fence was installed to justify allowing the workers who process fertilizer (a key component in many explosives) from not having to apply for a TWIC. Despite the objections of Congressman Jerry McNerney, the Coast Guard took no action to reverse the plan, the fence was installed making the Port's security worse—not better.

The ILWU representing the men and women who have built their careers working the waterfront, thank each of you for your commitment to our ports and we promise you have our full support in genuinely improving port security.

Chairman MCCAUL. Thank you, sir.

I now recognize myself for 5 minutes of questioning.

Let me share my concern about cybersecurity.

Mr. Seroka and I visited over lunch. I am very concerned about the attack that occurred last June. To echo again Norma Torres's bill we passed out of committee I think will help address.

I think you are absolutely right, we need to come up with a comprehensive strategy and plan to protect our ports.

I worry about the destructive nature of this virus and the attack. I don't think the press has really reported the severity of this. It is something that wiped out, you know, huge volumes of data, coming from a bank in Ukraine from a virus called NotPetya that very likely have emanated out of Russia.

A Russian attack on the Ukraine bank, the indirect victim is Maersk. Maersk gets impacted by the bank that they have. The virus gets into their systems, and then it impacts the Port of Los Angeles, having to shut down that terminal and then go to a manual procedure. Not to mention dozens of ports globally that were impacted by this one attack that got into the system.

I know the offensive capability of Russia, China, Iran, and North Korea. I think what happened in June demonstrates how vulnerable our ports can be to this type of cyber attack.

So, Mr. Seroka, to you, can you tell us the extent of the damage done and then what was done to repair that?

Then, moving forward, what can we do in Congress to help with the situation?

Mr. SEROKA. Mr. Chair, as you stated, the attack impacted one of our 27 terminals here at the Port of Los Angeles.

With the map to the side of you, that is the southern-most entity that you see, shaped like a sideways L. The A.P. Moller facility.

In and of itself would be the fourth-largest port in the United States; nearly 500 acres of land, 23 miles of roadway inside of terminal operation.

It is the pre-eminent facility that we have here at the Port of Los Angeles and arguably on the West Coast of the United States.

But it is important to note a couple of things. The attack that took place was pointed at, through a derivation of other efforts, at that particular company itself, not at the Port of Los Angeles as a whole.

The Port of Los Angeles in and of itself in use with that cybersecurity center has a domain of landlord operation here at the port. Simply meaning that we work with our private-sector customers to work here directly on that 7,500 acres of property.

What we saw immediately thereafter was our largest terminal shut down for several days. Then as they moved to a manual operation, moving maybe 10 percent of the cargo they normally would on any given day through this port.

They represent about 12 percent of the port's throughput today. The math from there becomes very significant.

The inability for the work to take place with Customs and Border Protection to clear the goods that come into the United States in the efficient electronic manner as designed was also thwarted. Simply stated, each container would have to be cleared on a manual basis by running that information over to Customs for evaluation.

So everything as we know it today was slowed down tremendously.

Your question then is, what can we do next? That is outlined in my written remarks as well as the testimony I gave here moments ago. It is three specific things.

Because this is such a private—public-private relationship between entities such as this municipality in the city of Los Angeles and its municipal agency, the Port of Los Angeles, the private-sector companies that work with us as customers every day, or lessees, long-term leases that average between 25 and 30 years to conduct operations here, and the necessity for those two groups to get together I think is job No. 1.

How can we compare best practices? More importantly, how could we share information of intrusion or potential intrusion that we have seen not only here locally but on a broader scale geographically?

Within that collaboration also rules of engagement, how we best can cooperate together.

I understand, not from Maersk specifically, but from other entities, that there may be some intrepidation on how Government's overreach in the cybersecurity center could be of some concern. I would like to have that bond work even closer.

With the cybersecurity center that we have employed since September 2013 here at the Port of Los Angeles, I advocate that we expand the fiber ring of that security center to be able to envelop the port's entity as its whole, that 7,500 acres.

How better we could work in response to the needs of the private sector without intrusion on their private and proprietary information.

I think that also takes money, and how we can better look at what money means to us today and how it goes downline.

I think it would be inappropriate for me to respectfully ask for a specific dollar amount today. But as we come to you with new ideas and new ways by which we can expand this fiber ring and create a more collaborative environment of sharing information through the Federal level down through our international counterparts and our customers, it will take some very creative looks at how we can model this, not only for Los Angeles and Long Beach, but how it will have impacts beyond.

But there is a lot of work to be done on the ground so we understand how better our role can be played.

Chairman MCCAUL. Thank you.

I look forward to working with you. Because you are correct, this was not a direct attack on the Port of Los Angeles, but the next time it could be. I think we need to be prepared for that.

Admiral, Mr. Martel, you know, the Navy has pulled out of the Western Hemisphere in terms of interdiction efforts, leaving the Coast Guard as the sole proprietor of that mission to protect the United States and its coastal waters.

Estimates are that one out of every three targets, you can only hit one out of every three targets. Which means two maybe getting in.

So my question is, well, first of all, if you can give me some, recognizing the space we are in, indication of things that we have

stopped that were a victory for the United States. But also, what is your biggest concern about what we are missing?

Admiral SOKALZUK. Chairman McCaul, I will talk first about what we have stopped. What we have stopped is a record amount of cocaine in the transit zone that is being attempted to flow into this country this year.

Although the fiscal year 2017 official numbers are not tallied yet, because that is a very specific process, just in the Eastern Pacific alone, we interdicted a hundred thousand pounds more than we did last year. I am quite sure that this year will be a record.

We were able to do that even though there is no Navy presence down there, all with Coast Guard assets, by the commandant strategy of concentrating Coast Guard ships in the transit zone and interdicting these in the Eastern Pacific.

One of the things that challenges us in that at this point, sir, is the state of our assets. That, in fact, one of the ships that you saw today was destined for that transit zone was unable to make it there the due to mechanical problems.

So the acquisition of the OPCs are very important for us to have more success on that. The—and the continued incredible performance of the National security cutters in the transit zone during the recent hurricanes. They actually ran some of intelligence operations down there that are normally done out of a major joint interagency center, due to the hurricanes.

So, sir, that is—we are only getting a portion of that. Some estimates 20 to 30 percent of the flow. So that can tell you how much is actually flowing into the country at this point.

Chairman MCCAUL. Mr. Martel.

Mr. MARTEL. Chairman McCaul, speaking from landside and within the port, we have interdicted quite a bit of narcotics in transit, freight remaining on-board, headed for Australia and Canada.

We have also worked with State and local partners in assisting in the interdiction of panga, maritime events that are landing along 200 miles of littoral border that I oversee as part of my area of operation.

I think the biggest challenge that we have in CBP landside are the marinas. We have over 90 marinas along the coastline that we have to patrol. We do not have the assets to operate outside of the port.

Chairman MCCAUL. Thank you.

My wife is pointing to Mr. Cordero. I agree with you on the UAS threat. My time has expired.

But I do think that is something the committee will be taking a look at in terms of right now as I understand it there are no restrictions. We know that—we have seen in Syria able to take these drones and turn them into explosive devices and chemical and biological weapons.

Mr. CORDERO. Well, thank you, Chairman.

I think coincidently this morning we were on the rooftop of the command and control center. The committee I think saw first-hand the potential threat when we viewed what seemed to be a super gigantic drone. Actually it was a one-man aerial craft in which, again, there is no restriction.

I think we see that the testimony you have heard this morning regarding not only the value of the cargo that comes into our Nation, which is a significant portion of our GDP in terms of the international trade as a whole, you know, you think about the worst scenarios of any damage to the infrastructure in this port, it is frightening.

So I do appreciate the committee looking into this issue and addressing as we go forward.

So, Mr. Chairman, thank you so much for raising that point.

Chairman MCCAUL. Chair recognizes Mr. Thompson.

Mr. THOMPSON. Thank you, Mr. Chairman.

Let me thank all the witnesses for their illuminating testimony.

One of the comments that ran through everyone's presentation was the notion that it is critical for the Federal Government to participate in this process of securing America's ports. Especially on the financial end.

Everything we had an opportunity to experience to date, so much of it was because of the Federal Government, either through FEMA grants or through other port security grants that are managed, that enable you to step up.

Sometimes we have tough decisions to make. But what I have seen here today says that the mission you have undertaken is a serious mission. We have to fund it. You know, second- or third-best toward addressing this mission is not good enough.

To that extent, we are challenged from the CBP standpoint to maintain a certain level of staffing.

Mr. Martel, are you able to maintain that? Or do you have some challenges with bringing new people in?

For the record, you know, we have had issues around the lie-detector tests that comes into play. We get told our veterans, who get out of the military with clearances, end up not being able to pass the CBP tests. They are holding clearances.

Would we reduce that reliance on lie-detector tests? Has that been helpful, or are you still waiting to see?

Mr. MARTEL. Sir, I think that is still under evaluation.

While we believe that the new protocol, the new direction we are using for the lie-detector appears to be a positive. I would have to get back to you as to what the actual results are.

What I can say here locally is from the Los Angeles field officer's perspective, we are adequately staffed.

We have not—we have implemented a number of new prototypes, technology, innovation, and whatnot to become more efficient so we could redirect staff to where we need them.

So we have not—again, we—I would say adequate. I would not say that we are overstaffed and that we would welcome additional staffing. But we have sufficient staff to effect our mission here locally in Los Angeles.

Mr. THOMPSON. I wouldn't expect you to say anything else.

Admiral, can you talk a little bit about the TWIC card as relates to the Coast Guard and whether or not the reference to some concerns about it and the reader mandate that Congress has put on you, whether or not you will be able to meet that?

Admiral SOKALZUK. Yes, sir, Congressman Thompson.

So the Coast Guard considers the TWIC card a very important component of our layered system of maritime security at this point.

I mean, there is no other standard antiterrorism background check that is being done.

In relation to the reader rule, the Coast Guard initially published the final rule last summer. Got some feedback from industry about concerns with the rule, confusion of how it is applied.

So we are taking a look at that, considering a possible delay in the rule. We are working through the rulemaking process on looking at the ultimate implementation of that rule, sir.

Mr. THOMPSON. Just one of the comments I would like to say on that is when TWIC was first envisioned, the notion was there would be one card that would allow a worker to get into a port.

But what has happened is every port has their own I.D. card in addition to the TWIC card. They ask for the same information.

So the notion is if we can eventually get to a universal card. But what has happened, as the port directors can tell us, that is also a revenue stream for local government, in some instances. Because you have to pay for the card.

So it is security, on one hand, but it is revenue on the other that gets plowed into some aspect of the particular situation.

So, Mr. Familathe, can you, since you had some issues with TWIC, do you have some better suggestions for port security workers? Are you saying we need to tweak TWIC?

Mr. FAMILATHE. I agree with your comment, and I like the way you said that. We need to tweak it.

We are not saying get rid of it. It is necessary to protect America's ports and the security of this country. We understand that is vital. But tweaking it so that it works for the workers is essential right now.

When there are small problems, the delays in the process, in going through all the hoops and—it is just not acceptable. Because a worker can't collect unemployment insurance. He can't go to work to feed his family. We would just like to see the process streamlined so that it works the way it should be.

Mr. THOMPSON. Well, the only other point I would like to make, Mr. Chairman, is everyone talked about partnerships. Now it is important, if we are going to get it right, everyone has to work together.

One of the things that put this committee together, Congress felt that if we are all in this together, we ought to be talking to each other, we ought to be training. Because we are fighting a common enemy.

So the partnership principle is absolutely essential for us to work. Old stovepiping of how we do things won't keep us safe.

So I compliment the men and women that I have talked to today on getting it right. But it is continuous training, it is continuous upgrading of equipment. All those things that will continue to keep us safe.

I yield back.

Chairman MCCAUL. Well said.

Chair recognizes Mr. Estes.

Mr. ESTES. Thank you, Mr. Chairman.

Mr. Martel, there are currently 61 Container Security Initiative ports in 35 different countries. You know, that is where we are doing some of the forward checks and starting the process on inspections.

Are there plans to add more CSI ports in the future? Do those plans also include having Customs and Border Patrol staffers or using local inspectors there?

Mr. MARTEL. Sir, I think we are always looking for opportunities to expand our footprint with regard to Container Security Initiative. Whether we have officers on the ground, whether we are working with foreign administrations and viewing inspections remotely, that is going to vary based on the footprint, the technology that is available.

But, in answer to your question, yes, I think we are looking to increase that where we can, where it is available.

The staffing footprint really will depend on the configuration, the logistics, and what agreements we have with the foreign government.

Mr. ESTES. Do we see better results from having our own forces there versus using local, or do we know enough yet to know we need a distinction?

Mr. MARTEL. Sir, I think it is—I don't know that we would make a distinction on that. I think when we are able to view things remotely, it is like having a person there. So our competence level that we have eyes on the container, eyes on the inspection, is the same as if we had someone there.

Mr. ESTES. Have you had issues or concerns with some of the—I mean, one of the things—I had an opportunity to go look at the Port of Rotterdam. One of the comments that was made in our decisions there was the biggest risk is somebody coming in and bribing an officer.

I don't know if we have that as a risk in some of the foreign countries more so that might affect this?

Mr. MARTEL. Sir, from our standpoint, all of the individuals that are involved at our CSR locations are vetted, especially the foreign service nationals, who are vetted by our local embassies there.

Sir, I would have to get back to you as to what our protocols are and what we think the risk assessment is. But our confidence level is pretty high that those issues have been addressed.

Mr. ESTES. Just to be clear, they weren't talking about that in terms of CSI, they were talking about in general what their experience was in the port, in general, and not anything in particular.

Admiral, can we talk a little bit about, you know, the inhouse cybersecurity capabilities that the Coast Guard has? Do you have capabilities that help you with those resources and that protection?

Admiral SOKALZUK. Congressman Estes, yes.

So first let me thank the Congress for the support and the fiscal year 2017 that helped us build our cyber protection teams and our cyber service provider resources in the Coast Guard.

So the cyber protection teams are really about defending Coast Guard networks at this point. Because if our networks aren't working, we cannot offer any, you know, perspective or assistance to anybody else. The cyber service provider group is more of a capa-

bility for recovery and routing, you know, bad things out of Coast Guard networks and that.

But Coast Guard cyber has provided us great perspective during some of the recent cyber incidents. That is always a resource for us to come and help industry.

I think one of the key things, as we talk about cyber in general, sir, is that we really have to instill a culture of cyber risk management. One of the ways we are doing that is in the area of maritime security committee meetings, which is exactly what some of the folks have talked about here, is sharing information, sharing the results of a vulnerability assessment, and making everybody aware of what you are seeing on your systems.

The Coast Guard recently published some guidance, the public comment period just closed on it, for cyber protection at facilities at this point.

Mr. ESTES. All right. Thank you.

Mr. Chairman, I yield back.

Chairman MCCAUL. Chair recognizes Mr. Correa.

Mr. CORREA. Thank you, Mr. Chairman. I want to thank Ranking Member Thompson as well for holding this hearing here in Long Beach because——

Ms. BARRAGÁN. San Pedro.

Mr. CORREA. San Pedro. Los Angeles and Disneyland. Covered all the basis.

Chairman MCCAUL. Got it all covered.

Mr. CORREA. Yes, sir.

But, you know, what I am reminded of is this asset. As I am hearing testimony and questions here from the committee, where can we invest the resources to be best used? What is the price? I am thinking to myself, what is the price of not being prepared?

Because, you know, the biggest port in the United States, all the commerce—I have just heard 40 percent of all imports, 30 percent of all exports of this Nation through this area.

What is it that we need to do?

So I guess my question would be, if there is one thing we need to invest in right now, what would that be?

Open it up to the committee.

Mr. SEROKA. From our side, I have been told by staff that there may be some that don't like the term "fusion center." We need to redefine, that is OK.

But what we see here immediately at the Port of Los Angeles is the need to formally bring in public and private-sector interests to do exactly what I mentioned earlier, share best practices, alert other partners of vulnerabilities, and have a systematic way of processing that information through expertise and the movement of data.

That would be the No. 1 ask.

I will get you numbers specifically off-line. We have been looking at that and talking with our Board of Harbor Commissioners specifically as to how we can quickly move out.

Second would be the expansion of that fiber ring I mentioned. The Cybersecurity Center that you toured earlier today, Congressman, shows an ability to capture data of potential threats or folks trying to find our weaknesses.

The ability to expand that ring, and that could be looked at as an analogy of just covering the entity of the entire port complex itself and allowing others to jump in.

Meaning could we be another firewall to those private-sector entities that are facing Congress every day and potential threats in and of themselves.

Mr. CORREA. I want to say that that is going to—love to hear your comments right now because that seems to be the theme that we have heard over and over again in our committee hearings on cybersecurity. Best practices, everybody working together, private and public sector, to make sure that everybody coordinates when it comes to cyber defense.

I want to thank you very much.

I guess another question to our folks at the Coast Guard and others.

Resources. You are severely lacking resources.

Defending the coast, defending our Nation.

Multipliers. We talk about working with our allies. Other folks have vested interests with us on security, economic issues.

Where do you suggest, what other agreements, what other nations do we need to approach in terms of working with us? Keeping in mind that we want to trust, but we also want to verify.

Mr. MARTEL. Sir, I will say from a CPB standpoint, we partner with other nations, other foreign customs services——

Mr. CORREA. Anybody else that we don't that we should be?

Mr. MARTEL. Sir, off the top of my head, no. I think that all of the partners that we have address our current and impending threats at the National level.

Locally, we work closely with HSI, with various task force State and locals to have connectivity with those countries that have a nexus, whether it be inbound or outbound, here at the Port of Los Angeles.

Mr. CORREA. Admiral.

Admiral SOKALZUK. You know, through the international port security program, we have engaged 150 countries. We visit those port facilities to make sure that they are exercising proper physical security procedures. We will begin to look at cyber. Because we just consider that another way that we have to manage risk in the port at this point. So I think that has been very successful for us.

I think that from a—from an information exchange point, as I talked about earlier, the area maritime security committees that here locally in the country, of course, most of them at this point have a cybersecurity subcommittee where we have a lot of these discussions and exchange a lot of that information.

I will just recognize too some of the—I will recognize A.P.M. Maersk, Mr. John Ochs, who came and spoke at the Area Maritime Security Committee, was very candid about what A.P.M. faced in that particular attack.

Just in terms of resources, obviously, you know, it will take resources to do some of these things as we understand cyber threats. As they evolve, all of our systems are becoming more complicated, so we will have to be willing to make investment.

Mr. CORREA. Mr. Chair, I yield.

Chairman MCCAUL. Sticking with committee Members as a priority, Ms. Barragán is recognized.

Ms. BARRAGÁN. Thank you. I want to thank you, Chairman and Ranking Member, for holding this hearing in my district here in San Pedro to examine security at the Port of Los Angeles, or as we like to call it here, America's port.

Thank you to all the witnesses for your work and for being here today to provide testimony and your perspectives.

You know, the Nation is just facing evolving threats constantly. When I came to Congress, it was important for me to seek an appointment to this committee because of the importance to the homeland and to the ports, which is by far the largest economic engine in the region and touches every Congressional district.

So it makes me really happy to be here today to have this hearing. So thank you, Mr. Chairman, for doing that.

Before I get to my questions, I have some statements I want to enter into the record from local groups and individuals concerning security at the Port of Los Angeles.

Chairman MCCAUL. Without objection, so ordered.

[The information referred to follows:]

COMMENTS FOR THE RECORD SUBMITTED BY HON. BARRAGÁN

COMMENT 1 OF 4

Carlos Garcia

A real homeland security risk to the Ports of Los Angeles and Long Beach lies at their "back door" and is not addressed by the Coast Guard and Customs or the Port of Los Angeles to the best of my knowledge. The risk lies at the Rancho LPG facility where two 12.5 million-gallon refrigerated butane storage tanks are located in San Pedro less than 0.25 mile from the Port of Los Angeles. The facility is located on private property not under the jurisdiction of the California State Lands Commission or on land under the Port of Los Angeles' jurisdiction. However, the Port does have an ownership interest in the railroad spur track which serves the Rancho LPG facility.

The risk posed by a terrorist attack on the Rancho LPG facility is significant. If the facility was attacked and one of the tanks ruptured, liquid propane would be released and evaporate in the ambient air. When an ignition source is encountered, possibly from one of the three back up gas compressors on-site or even a spark from a passing car, there would be a vapor cloud explosion. Using the TNT equivalent calculation methodology in CFR guidance (40 CFR Part 68), the impact radius would be about 3 miles in a worst-case scenario. According to a September 2010 Cornerstone Technologies report, such an explosion would cause large-scale structural and physical damage due to the rapid overpressure caused by the explosion. The impact would encompass terminals in Long Beach and include nearly all of the terminals in the Port of Los Angeles and the Los Angeles Cruise Terminal as well as the visitor-serving areas of the proposed San Pedro and Wilmington Waterfront projects.

There are also five horizontal bullet tanks located near the larger butane tanks each capable of holding 60,000 gallons of liquid propane under pressure on the Rancho LPG facility. They might also be compromised in vapor cloud explosion that ignited the pooled liquid butane leaking from one of the larger butane storage tanks. The burning butane would be hot enough to melt the bottom of the steel pressure vessel tank resulting in explosion of the propane tank in a boiling liquid vapor cloud explosion (BLEVE).

There are numerous Federal, State, and local agencies that regulate the facility besides the Department of Homeland Security including:

Federal:

- U.S. Department of Transportation
- U.S. Environmental Protection Agency
- U.S. Defense Logistics Agency
- U.S. Department of Occupational Health and Safety Administration

State:

- California Environmental Protection Agency
- California Emergency Management Agency
- California Department of Toxic Substance Control
- California Department of Industrial Relations, Division of Operational Safety and Health
- South Coast Air Quality Management District

Local:

- Los Angeles City and County Fire Departments, as the designated Certified Program Agency
- Los Angeles Police Department
- Los Angeles Emergency Management Department
- Los Angeles City Attorney
- City of Los Angeles Bureau of Sanitation Industrial Waste Management Division
- City of Los Angeles Department of City Planning.

However, I am not aware of any coordinated efforts at the Federal, State, and local levels to mitigate the physical security vulnerabilities posed by this facility described above. I doubt that any of the hearing witnesses will address these risks.

I believe that these risks should be evaluated by the Department of Homeland Security in addition to seaborne threat scenarios addressed by the Coast Guard, Customs, and the Port of Los Angeles. The Rancho LPG storage facility represents a much easier target than the seaborne threats that will probably be the focus of the October 30 field briefing on port security.

COMMENT 2 OF 4

Janet Gunter and Chuck Hart, San Pedro Peninsula Homeowners United, INC.

October 30, 2017

The Ports of Los Angeles and Long Beach represent significant & documented targets of terrorism due to their surrounding population densities, their massive employee work force, and the number of concentrated ignition sources, including chemical and fuel terminals. These facts highlight the prime opportunity for terrorism to cause extraordinary loss of life and extreme infrastructure damage resulting in financial collapse of the U.S. cargo industry. Many of us well understand this.

The issue that stands above and apart from this public understanding . . . in its "inexcusable" state of existence . . . is the Plains All American Pipeline/Rancho LPG storage facility, storing in excess of 25 million gallons of highly explosive liquefied petroleum gases, on the precipice of the Port of Los Angeles. This single site offers any terrorist the "mouthwatering invitation" to strike. With a single one of its two 44-year-old tanks having a blast radius of over 3 miles, the opportunity for devastation is pure "gold".

On September 11, 2014, Congressman Waxman's office hosted a public meeting on the Plains/Rancho LPG facility. Mr. David Wulf, director of the DHS Infrastructure Security Compliance Division, publicly acknowledged that the Plains/Rancho LPG facility is a "Tier One Soft Target of Terrorism". The antiquated tanks of this facility are readily accessible and can be easily ruptured by either a high-power rifle or rocket-launched grenade. Considering the recent actions of the Vegas shooter and his direct aim at nearby fuel tanks in his attack, we are given additional anxiety by this LPG tank target potential. We are talking about an explosive and cascading inferno potential that is extraordinary in its scope.

Both expedited and exempted from numerous permits and regulations by the Nixon administration in the early 1970's, this facility was introduced solely as a "storage" site for LPG received via pipeline from Algerian ships calling at Berth 120. This was envisioned as an "emergency" action necessary for back-up energy supply under the false notion that the import of this commodity would wean America off of foreign oil. Both Nixon's political demise and the explosive nature of this gas, eliminating it as a broadly-used energy source, caused the original Petrolane LPG facility to go bankrupt. In the 1980's, instead of the port and city of Los Angeles welcoming the opportunity to remove the already well known high-risk potential of this site, they embraced an entirely "new" business venture for the successor. Taken over by Amerigas, a pipeline was installed to Ultramar refinery (now Valero) several miles away in Wilmington for the expressed purpose of "off-site storage" of the facility's "most" hazardous commodity, butane gas. That pipeline was later tapped into by BP (now Tesoro) refinery in Wilmington to also transport their own butane for storage. This use was "never" anticipated nor reviewed in the highly-deficient EIR performed for the initial project. The existing business operation is "entirely" dif-

ferent. While a rail dock is mentioned in the EIR of 1973, there is no analysis of rail use, whatsoever. Both the rail and pipeline uses, which now currently traverse both under and over port public trust lands, have never considered the volatile nature of this gas nor identified its associated risks and liabilities. In 2008, this facility was purchased by the Plains All American Pipeline company and is operating as a Limited Liability Corporation under the name, Rancho LPG LLC.

Sadly, since the DHS publicly announced the high risk of this site in 2014, we have yet to see any responsible action. Opportunities abound to affect change to eliminate this highly dangerous risk exposure at multiple levels of government. The function of the Plains/Rancho LPG facility depends "entirely" on the use of public trust lands to facilitate its operations. Without those assets, there is NO business conducted at Rancho LPG!

The Surface Transportation Board ruled last March that the "local government" has the right to "policing of safety" on the use of the Port's own rail. Our Federal legislators should be leaning heavily on local Government officials to enforce this right and protect the innocent and our ports. The "use" of the pipeline under public trust lands falls into the same category. California State Lands Commission also has an obligation to the people of our State as guardians of the public trust. The DHS charter states the following: "Whereas the Department of Defense is charged with military actions abroad, the Department of Homeland Security works in the civilian sphere to protect the United States within, at, and outside its borders. Its stated goal is to prepare for, PREVENT, and respond to domestic emergencies, particularly terrorism.

We urge immediate action on this issue by the leadership. The consequences of not responding are far too great to ignore any longer.

Sincerely,

JANET GUNTER,
Member SPPHU.

CHUCK HART,
President SPPHU.

COMMENT 3 OF 4

Marcie Miller

October 30, 2017

The U.S. Department of Homeland Security asks everyday citizens such as myself, "If you see something, say something."

Today I am saying something and I hope Homeland Security is listening.

The U.S. Department of Homeland Security has long been aware of the dangers of storing and transporting ultra-hazardous chemicals. Forty-five years ago politicians and safeguards failed this community by enabling Petrolane to build—with the assistance of the U.S. Government—the bulk storage facility known today as Rancho LPG, LLC.

Adjacent to a pre-existing community of people and places of commerce; at the Nation's largest and arguably most important port of entry; on unstable landfill; in a known seismically active fault zone; in a methane zone.

The inappropriately located Rancho LPG bulk storage facility remains as a reminder of just what a homeland security failure looks like. So now a new generation inherits this ticking time bomb, despite the unanimous consensus that the risks are unacceptable.

Oil and gas industry lobbyists and paid consultants knowingly play down the likelihood of catastrophic risks. Yet, we know the unthinkable is possible; we witnessed that at Fukushima and at countless other ultra-hazardous biochemical disaster sites. If you choose to do nothing, you will abdicate your responsibility to protect this State's greatest resource—people.

What can you do?

1. Please, determine that human life is more important than corporate greed;

2. Remove politicians and lobbyists from the determination process;

According to the city of Los Angeles Ethics Commission, over the last 10 years, Rancho LPG, LCC has donated over $22,000 to local politicians, including current Councilman Joe Buscaino; previous Councilman and current Rancho lobbyist, Rudy Svorinich; and just days after rendering a decision in favor of Rancho LPG, LLC, L.A. City Attorney Trutanich received a large contribution to the "Trutanich Office Holder Committee 1301975" from Plains Marketing, LP on 2/25/11.

Rancho LPG, LLC has donated handsomely to EastView Little League, an organization synonymous with sitting two-term Los Angeles Harbor Commissioner, An-

thony Pirrozzi, long-time league president, member of the steering committee, and coach.

In 1977, Gov. Jerry Brown tasked the California Public Utilities Commission to inspect the marine terminal of Petrolane, Inc. to determine its potential hazard to the surrounding area. Despite his acknowledgment of the high risks associated with the siting of this ultra-hazardous facility, his final report concluded only that,

"The city of Los Angeles Department of Building and Safety has determined that Petrolane's low temperature liquefied petroleum gas (LPG) units are not exempt from Section 91.0102 of the Los Angeles Municipal Code as originally indicated. Accordingly, on April 20, 1977, the department issued an order to comply to Petrolane, Inc., which directs the company to file plans and obtain building permits for the two low temperature LPG storage tanks. The review will include a check to ensure their ability to resist seismic loading."

Needless to say, the seismic issue has remained. Had the original Petrolane facility been subject to SEC. 91.0102., it could never have met the requirements of the code, the purpose of which was,

" . . . to safeguard life, limb, health, property and public welfare by regulating and controlling the design, construction, quality of materials, use and occupancy, location and maintenance of all buildings and structures erected or to be erected within the city, and by regulating certain grading operations within the city."

It is important to note that this section of the Los Angeles Municipal Code was replaced in November 21, 1989 by Ordinance No. 165310, which deliberately elevated the safety bar not only for new construction, but also for "alterations" and "repairs."

" . . . Where, in any specific case, different sections of this code specify different materials, methods of construction or other requirements, the most restrictive shall govern. Where there is a conflict between a general requirement and a specific requirement, the specific requirement shall be applicable."

It should come as no surprise that Governor Brown received substantial campaign donations and questionable loans from the Petrolane company.

3. Act swiftly to correct past failures and mitigate dangers before the unthinkable does happen.

In 2007, the "Department of Homeland Security Appropriations Act of 2007, mandated that the Secretary of the Department of Homeland Security establish risk-based performance standards for the security of high-risk chemical facilities within 6 months of the enactment of the Act. Also mandated was the development of vulnerability assessments as well as the development and implementation of site security plans for high-risk chemical facilities. The CFATS interim final rule was promulgated to fulfill the requirements of this Act."

Why has Homeland Security done nothing to protect both people and property from the profoundly high-risk chemical facility casting a grim shadow for miles in every direction?

Further evidence of risk-based performance threats to homeland security are records collected by the California Public Utilities Commission regarding the staggering number of train derailments along the Pacific Harbor Line, which transport these chemicals throughout the Port of Los Angeles and the San Pedro/Wilmington communities.

Although the Pacific Harbor Line has a fine-tuned public relations strategy that toots a loud bullhorn about its attention to safety, the truth is, CPUC documents a jaw-dropping 40 derailments between 2008 and 2012! I have contacted CPUC numerous times to obtain 2013–present records but never received a response. Simply based on this unacceptable derailment record, the Homeland Security Appropriations Act of 2007 mandates immediate intervention to cease and desist all Pacific Harbor Line operations

Why has nothing been done to mitigate this risk???? Why are regulators not all over this??? These facts must be known. Thank you for reading my concerns and, hopefully, for changing the course of history.

COMMENT 4 OF 4

James Dimon

Having looked at the current situation with Port of Los Angeles (POLA) security and their relationship with law enforcement which surrounds the port complex the following has been determined to be a necessary component toward POLA and community safety.

We believe by ensuring Los Angeles Police Department, Harbor Division is equipped with license plate reader technology it would add an important layer of security to the port complex extending miles in some cases from its shores.

This technology is already being utilized by surrounding communities like Rancho Palos Verdes and should include participation by the Los Angeles Port Police as well.

We also believe a pact of cooperation should exist with the implementation of this technology, stressing the importance of different agencies to sharing critical safety information with each other, thereby increasing the effectiveness of the system and the security of not only POLA, but that of the citizens who reside on its boarders.

The technology is proving to be highly effective in identifying intruders into the city of Rancho Palos Verdes alerting law enforcement before they can act and as an increasingly valuable investigative tool.

POLA is currently bringing millions of people to the Complex utilizing existing infrastructure. POLA's expansion projects are working to improve that infrastructure that will bring millions more in the future. Plans for the San Pedro Market Place, Alta Sea, Banning Shores and the Avalon Blvd expansion will undoubtedly increase the desire to come down to the Port Complex.

In closing we need to be proactive with our approach to addressing what will be increased security of POLA and the surrounding communities. Here is an opportunity to get ahead of the security issues with a police division which is tops in the country practicing law enforcement.

Please consider the importance License Plate reader technology would provide toward a huge boost to Port Security and that of its neighbors.

Ms. BARRAGÁN. Thank you. So statements are from groups like the San Pedro Peninsula Homeowners United, Mr. James Diamond, and Carlos Garcia. They offer the committee an often-overlooked local perspective as we consider port issues.

Mr. Familathe, thank you for raising the issues with the TWIC program. This is something I have heard not just from your organization but from others. The concerns on what the program does or doesn't do and the burdens it imposes.

We always want to make sure that we have security at the forefront. So I am hoping that we can work in a bipartisan fashion to address some of the concerns that were raised here today. So we have a lot work to do on that.

Now, for my questions, I know that Mr. Martel indicated that the staffing was sufficient.

Mr. Familathe, you are on the ground. Your members are on the ground. You handle the cargo. In your perspective, given that your members are there and you see first-hand, but do you believe that the current CBP staffing levels at the ports are adequate?

Mr. FAMILATHE. No, I do not.

Our members work 7 days a week. There are only a few no-work holidays throughout the entire year. With pressures to move cargo 7 days a week through ports like Los Angeles and Long Beach, it is important that not only the longshoremen are there. We can get the cargo off the ship. But if CBP doesn't have it budgeted to have that staffing on the weekends and the CBP officers there to X-ray the cargo, then we can't keep that cargo moving.

So it works hand-in-hand.

We would really like to see the proper budgeting.

They may have the staffing. I won't challenge Mr. Martel here on that. He knows his operation better than anyone. But maybe they don't have it budgeted to have those CBP officers working weekends.

Ms. BARRAGÁN. Certainly, we will follow up on that.

Mr. Cordero raised an issue that I get asked about all the time. That is, do a hundred percent of the containers and the cargo that come into the port get scanned?

Mr. Martel has indicated that a hundred percent get the radiation scan, but only the high-risk get the X-ray.

My question is does the fact that we don't X-ray 100 percent, knowing that Mr. Cordero said it was impractical, does that leave our port at risk?

Mr. MARTEL. I don't believe that it does.

I think we have a very robust targeting system. We are able to get information as part of the 24-hour advance cargo manifest rule, we are able to get cargo information 24 hours before the cargo boards a vessel.

So we have a unique opportunity to scan the commodity, look at all of the shipper/consignee information, bounce it against various Classified law enforcement databases, trade databases, open-source information, to do an in-depth assessment as to whether or not the cargo presents a threat.

Ms. BARRAGÁN. Thank you.

Mr. Seroka, I want to ask you about an incident that happened in the fall. You may have—I am sure you heard about it—the high-speed chase that ended here at the port complex. It ended up with the suspect climbing a large crane and even at one point passing two workers on his way up, before ultimately falling to his own death. It was an unfortunate incident.

I think a lot of us were surprised that a car could get onto the port and to do this. I often think about bombings. What we do today is we put up these barricades so cars can't get past. That this gentleman was able to access the port complex as easily as he did.

Can you tell us what additional security procedures have been put in place as a result of this? Because of my concern that it could pose to homeland security.

Mr. SEROKA. If I may, Congresswoman, it would be helpful I think to the committee to start with a wider context of this specific incident.

The alleged assailant stole a car from a dealership in the Inland Empire, approximately 60 miles away from the port. Moving through multiple counties with various jurisdictions of pursuit, the driver was moving through our network of surface streets and freeways in a very erratic manner. Insomuch that leadership of these agencies had moved closer and then decided to retreat from this particular driver, not to impede upon the public's safety.

The driver then approached the harbor area on the 110 Freeway. All throughout this police chase that went through multiple counties, we had no indication that this driver was targeting or set to enter the port complex.

After weaving his way through several street and local neighborhood enclaves, a U-turn was made to go back onto the 110 Freeway and take an immediate exit off of that freeway toward port property.

From all accounts, both on-site as well as in the air, as this was telecast by local news on multiple channels, the driver began to follow traffic and turned in to a specific terminal that was led in by ILW work force that was going to work for the nightside shift.

That is a traditional gate that will be open to our workers so they can get on-site with safety and move to their jobs beginning at 6 p.m. The penetration was made at approximately 5:50 in the evening.

Getting onto the terminal site was met with response from our Los Angeles Port Police unit within 3 minutes and 20 seconds of notification of that breach.

Once on-site, there were a number of tactical details and protocols that needed to be followed, especially through the allied agencies, and the necessity of highly sophisticated response teams that were called to that particular site once Port Police had cordoned down the situation.

It is unfortunate, but that individual did climb a crane and either fell or jumped to his death.

What we have done in the timing since then, although none of this could have been predicted, is that we fortified gate activities, not only at that particular facility, but also created different paths of cargo entry as well as personnel and visitor entry with credentialed folks that will be working on the port.

In addition, all of these standards at the particular facility that was breached and others that we immediately took under evaluation were at or above United States Coast Guard standard for entry and exit.

But we will continue to raise the bar on that in collaboration with Coast Guard, CBP, and other allied agencies to make sure that our threshold goes well beyond that is mandate.

Ms. BARRAGÁN. I yield back, and I apologize for going over.

Chairman MCCAUL. The Chair recognizes Mr. Rohrabacher from Orange Country.

Mr. ROHRABACHER. It is good to be back. Some of you may not understand, but I represented this area for about 10 years. Mario and I worked out a lot of problems together. But it took a lot of work to do it. I tell you that much.

We have—you know, this port is one of the great assets of our country. As such it has got special considerations that we have to look at. I know as the 1900's turned into the 20th Century, we faced certain challenges. I happen to have observed the changes that were taking place when we went from having everything in boxes and taken off the ships in boxes, and longshoreman would have to take them off individually.

The great cost and actually cooperation that was necessary to create this new system that we have, or the system we have now, of containers, which is basically so efficient we have developed what would be a conveyor belt across the ocean. That is how efficient we are.

Well, a lot of people are taking advantage of that conveyor belt to make money. That is what they should do. We have a market system here. People looking for profit.

But I would hope that as we look at the new challenges that come with this change of technology that we make sure the people using the conveyor belt help pay for the things that we need to do to make sure that that economic conveyor belt stays in process.

Mr. Lowenthal and I have been really involved in that issue for a long time. We still are active in this.

So as we are looking at some of the things, Mr. Chairman, that need to be done to keep this system safe, which is what we are focusing on today, but also functioning, let's make sure that we work together, but we take the approach that those profiting from this new system will pay the bill in devising ways of making it work better.

These new challenges, Mr. Chairman, that you focused on today, thank you for being here to help us discuss those.

The cyber attacks. Let me know—I am on the Science Committee, and even I have a tough time in figuring out how these cyber attacks work. Today with the testimony that we have had, it has been very beneficial to me and I am sure to all of us to think how we can deal with this. We have already—we have got an example now.

We know, over the years, as I say, since I represented this, we know that even when there is a slowdown here, it costs hundreds of millions of dollars just to have a slowdown. If there is a cyber attack, it shuts the whole thing down even for a couple days, it is an economic catastrophe. Thus we do need to work together to see what we can do to head off those problems.

We talked also today, someone mentioned drones.

Well, we never had to worry about drones 20 years ago, did we? But, yes, that is something we are going to have to think about. Think about what the penalties should be, what the rules should be.

I want to ask, Mr. Chairman, someone mentioned overreaching. That we can't be overreaching in cyber. Which one?

Mr. SEROKA. I mentioned that, and that is not exactly what I stated.

Mr. ROHRABACHER. Could you give us a note of caution of not going too far so that if we are trying to make the system safe that we don't freeze it.

Mr. SEROKA. I mentioned in my earlier question and answer back to the Chairman that as my recommendations and that of our department here, which is a municipal agency in the city of Los Angeles, that I felt there were a couple things we needed to do. One was that collaborative spirit of bringing people together, sharing information systematically——

Mr. ROHRABACHER. What about overreach? Where does that come in?

Mr. SEROKA. As I stated on the record that there are some in private-sector industry that feel that Government may overreach. As we get into those areas, we need to have a sensitivity toward that.

Being on the ground here and coming from the private sector, I think I see a lot of those sensitivities and can help find those unique aspects that we can work together.

Mr. ROHRABACHER. So in other words——

Mr. SEROKA. We have to be mindful of that.

Mr. ROHRABACHER [continuing]. What we have got to do is we have got to make sure we are taking care of the problem but not so much that we are killing the patient when we are trying to correct the disease.

So that is my only admonition—two admonitions. No. 1, let's find ways of paying for it by the people who are making the profit on

this conveyor belt, and, No. 2, let's make sure we don't overreach so that we are actually becoming the enemy and slowing down this great wealth-producing enterprise that we have here in our ports.

Thank you, Mr. Chairman, for coming and joining us today.

Chairman MCCAUL. Thank you for being here.

Excellent point with respect to overreach. The cybersecurity bill we passed out of committee—it is law now—was predicated on the Department not being able to regulate. Because we thought to have a true information-sharing relationship, you are not going to share information with some entity that can regulate your industry.

I think providing the liability protection even went further so that, you know, the financial institution here can share with the other one without threat of a lawsuit.

So I hope that is working. It has been a great experiment. But the threat is very real.

So thank you for that.

Mr. Lowenthal.

Mr. LOWENTHAL. Thank you, Mr. Chairman. Thank you for inviting me.

It is really an honor, as the person who is the co-chair of the Ports Caucus in the Congress of the United States and also as the representative of the Port of Long Beach, cybersecurity is not an area that I am proficient in. So for me this has been a great experience, just listening.

But I want to get back to, you know, we have a lot of conversation or much of the conversation focused on the impact of the cyber attack in June of this past year to Maersk.

When I spoke to Maersk about that right after they said, you know, they are going to be able to cope with it and live with it. They didn't like it. But they had the resources.

But they also indicated to me that they were not alone. There were a lot of smaller, you know, lines that were also impacted in other ships. It is not just the large people.

So I want to get back to the Coast Guard.

You know, with this attack, which I believe occurred off the Black Sea, and there were over 20 ships that lost their GPS systems. Researchers have indicated now, I believe, that there really are software vulnerabilities in commonly-used communications and navigation systems on cargo vessels and tankers, et cetera.

I would like to know from the—if there are these vulnerabilities, not just for the large ones, and the large ones were saying we will live. We don't know how the smaller ones that were impacted are actually going to be able to exist, you know, and whether they—the question is, what is the Coast Guard—are you aware of that right now in our system that is out there, we have these vulnerabilities?

Maybe the large companies will be able to fix it, but what are we going to do about this? Does the Coast Guard see this as a tremendous vulnerability that is out there?

Admiral SOKALZUK. Congressman Lowenthal, thank you, sir.

I think the Coast Guard does see this as a vulnerability. We have had several instances now, this Black Sea incident that you referred to.

Mr. LOWENTHAL. That is right.

Admiral SOKALZUK. Those ships figured out what was going on through use of relying on their training to IMO standards and things like that, figured out that their GPS signals were not indicating the right thing in their position systems.

I think as these electronic systems become more interconnected, we will see more of that.

I think, you know, one thing that we have to realize in a lot of these stems is the human in the loop has to work well, has to be well-trained, has to understand some of this. We have to look at all these systems and build that resiliency into there that somebody has other ways to verify the operation of a system.

In this case, it was training for them. They probably had visual aids to navigation or something like that. Just like in this country, as you approach the ports, you don't completely rely on GPS, you start to rely on the visual aids to navigation that the Coast Guard maintains.

But we worked with IMO and industry to develop guidance that takes cyber into account into safety management systems for ships. So there is an IMO circular out on that right now, sir.

But we have to continuously identify these risks and really instill this culture of constantly evolving how we manage risk in cyber. But ultimately there has to be, you know, resiliency and redundancy that people can rely on. It is oftentimes humans and people with good training.

Mr. LOWENTHAL. I want to follow up—thank you for that answer—something that Mr. Martel talked about, and I think you—and when you were talking about your advanced information systems that you get about what is taking place, it just triggered to me a conversation that I had with Mr. Seroka recently about the ability or the need to kind-of coordinate all the digital information and really understand not just a day or two before a ship is coming, but exactly what is happening and to be able to share that information.

So I really want to say to follow up to ask Mr. Seroka, how can—what are the improvements that we are already beginning to see in the information systems technology and how can that help us with the cybersecurity?

Mr. SEROKA. Yes, Congressman. You are referencing a discussion we had about one of our signature initiatives here at the Port of Los Angeles, the Port Optimizer, or Information Sharing Portal.

Mr. LOWENTHAL. Yes.

Mr. SEROKA. That was co-designed between General Electric Transportation and the Port of Los Angeles.

Mr. LOWENTHAL. I believe the Port of Long Beach is going to soon be part of that system also.

Mr. SEROKA. We are very hopeful. Yes.

Executive Director Cordero and I have been speaking about those opportunities regularly as to who we could really work together in this area.

Mr. LOWENTHAL. I encourage that.

Mr. SEROKA. Thank you.

Dating back about 3½ years ago, Congressman, you will remember the depths of congestion that we witnessed not only here in southern California, but throughout most of the world's east/west

trade gateways due to dislocations in the supply chain, new partnerships that were being formed, the unfortunate financial travails our maritime community had been facing since the advent of the recession, and other causes.

We felt at that time that if we could do a better job sharing information across stakeholder groups we could find operational efficiencies that would be necessary to bring this port complex and others not only to standard but beyond that for what our customers expected.

So we began working with—with customs and specifically Mr. Martel, along with others in Washington with the Department of Homeland Security and CBP, Rich DiNucci, to be specific, who offered ideas on how we could utilize information through the Customs Advanced Manifest System, which Mr. Martel referred to earlier, is a vetting process used 24 hours between vessel sail from Asia here to the United States.

My ask was pretty simple in that I wanted to utilize generic information. I did not want to know what was inside the container, how much it cost, or any other sensitive or proprietary data that Customs may hold.

The point of bringing General Electric on was one of a company who has a great reputation of being a steward of information, and holds many Federal, State, and local contracts throughout the Nation.

That information now in its earliest stages has been tested here at the Port of Los Angeles and with the permission of Board of Harbor Commissioners will be rolled out to the entirety of the port over the coming months.

The idea is that the earlier line of site we have on this information the better we can mobilize our service providers and partners to move the cargo and its conveyance system in a much smoother way.

Having earlier access to that data will also show, potentially, any abnormalities so this group of trusted partners can again convene and talk about what we can learn from those and how best we can protect our interests of our assets, people, and the cargo that moves through our port.

Mr. LOWENTHAL. Thank you.

As I yield back I also want to agree with Congressman Rohrabacher that we definitely need a sustainable revenue stream to enhance the movement of goods.

Thank you.

Chairman MCCAUL. The Chair recognizes gentleman from San Diego, Mr. Duncan Hunter.

Mr. HUNTER. Thank you, Mr. Chairman, and thanks for being here. San Diego.

Let's start with this. The Chairman hasn't talked about it. But he has got a book called "Failures of Imagination." Did I get that right? "Failures of Imagination." It starts off with a pretty catastrophic attack in the District of Columbia. But it goes through things we haven't thought of yet.

So the containers, where everybody is checking those, if there was one failure of imagination, something you that haven't thought about yet today, what is it? It is a big yacht that blows itself up?

What would be our failure, sitting here, after something bad happening?

Because we are checking out containers all the time now. You are focusing there. So if I was a bad guy, I would sure as heck not do anything on a container. I would do something else. Talked about we stopped using panga boats. We are now using recreational boats more. Right? Because they don't get flagged.

Anyway, what is a failure of imagination here?

Mr. CORDERO. If I may, Congressman, says that is a great question.

As I note in my testimony, part of the concerns or issues we were going to address is what are the new threats? To the question.

The unmanned aircraft is that new threat. I mean, because when you start talking about the potential, what could happen, a catastrophe.

I think, on the other hand, if we are proactive and make sure we approach this issue in a way that the port authorities would have the ability to restrict usage of the unmanned aircraft and/or drones as we know it, then of course it certainly would mitigate that type of threats.

Mr. FAMILATHE. In my testimony that was submitted, ILW used to inspect all the containers coming out of the waterfront. As the industry changed, cameras were installed at the gates in the terminals.

We no longer open doors on containers. We know how vulnerable we are in this country from within. Empty containers are parked on the street. Truck drivers pick them up, bring them into the terminals. I believe that that is a huge vulnerability for us.

When our guys used to open the doors, you could see if anything was inside. Now that doesn't take place. A camera is looking up top, but you are not seeing inside the container, of all the containers, of particularly a small port like San Diego.

Mr. HUNTER. Thank you.

Gentlemen.

I have got one more question too. So we got UAS not looking inside containers.

Yes, Admiral.

Admiral SOKALZUK. So, Chairman Hunter, what I would say, sir, is I think we have got to put that imagination into our exercises. Make sure that we fully explore things like when we have an incident, like some of the things that we have just had, where we are operating on backup systems and we are doing things manually that somebody can't do something that gets something through into this country.

No matter what realm it is, whether it is within Customs' realm or the Coast Guard's realm, I think we have got to inject a lot of imagination into those exercises and really look at that particular piece when we are operating in manual mode.

Mr. HUNTER. Thank you.

Mr. MARTEL. Sir, I would echo the admiral's comments.

I would also add to your point. Private vessels, pleasure craft continue to be a challenge for us. You know, I think we need to strive to have better domain awareness of our responsibility. That

is presently, you know, one of the challenges here locally within Los Angeles.

I think working through the AMSC, through our regional coordinating mechanism, working with all the State and locals, getting out there and working with harbormasters and whatnot is part of our plan. It is what we are currently doing, to try to have more visibility as to what that threat is. But that continues to be the unknown because those vessels come in and out daily.

Mr. HUNTER. Thank you.

Last question. Try to do it in 1 minute.

What percentage of the port or of the terminal operators are foreign-owned in Los Angeles and Long Beach?

Mr. SEROKA. Ninety-eight percent?

Mr. HUNTER. Are foreign-owned.

Mr. SEROKA. Yes.

Mr. HUNTER. Who approves who owns them?

Meaning, can the Iranians operate a terminal? Can the Iranians—can somebody—can Pakistan operate a terminal? Or are they all happy countries that operate——

Mr. SEROKA. No. That would be a situational awareness with respect to how the vetting process goes with respect all the way down to municipal——

Mr. HUNTER. Ninety-eight percent of the ports.

Mr. SEROKA. Similar circumstances.

Mr. CORDERO. Yes, that is correct, Congressman.

I would also say that the CPS process right now that is in the District of Columbia certainly addresses those issues. Of course that process specifically addresses the security threats with potential transactions.

Mr. HUNTER. Does CBP look at a terminal operator differently if they are—let's say that they are—name a good country; I don't want to say if there are good or bad countries because we are all wonderful.

But let's just say a Western civilization, first-world country, versus Iran.

Do you look at the normal operator differently if it is owned by different types of folks?

Mr. MARTEL. Sir, that I would have to get back to you on in terms what we do at the Coast Guard.

Mr. HUNTER. You do game theory. That is how you determine what targets to go after to pick.

Mr. MARTEL. Yes.

Mr. HUNTER. I would have to play into there. Right.

Admiral SOKALZUK. Congressman Hunter, I don't think we look at them differently. We enforce the same standards on them for facility security, facility security plans, facility security assessments, unannounced spot checks. All those things.

So I think that rigorous approach, while I am unaware that we have ever modified it for a certain national terminal owner, I think that is what really helps us maintain security in the port is that regimen.

Mr. HUNTER. Thank you.

I yield back.

Chairman MCCAUL. Good points.

Thanks for the plug for my book as well.

But I think imagination is important. Red team exercises to keep, you know, finding vulnerabilities. I think the cyber event demonstrate a vulnerability that we can hopefully make better.

Mrs. Torres, is recognized.

Mrs. TORRES. Thank you, Mr. Chairman. Thank you again for inviting me to participate in this very important hearing right here in California, the Port of Los Angeles.

I want to also thank Ranking Member Thompson and both of your staffs for helping me with my bill. Certainly, we could not have been able to get it through the committee without your assistance of your staffs and all of the commitment that we have seen today from the Members of the committee. So thanks again for that work.

Going back to a comment that you made earlier today as we started this conversation, Mr. Seroka.

The attack pointed at the company when we were talking about this last cyber attack in August. I forget.

How can we not think that the attack was not necessarily targeted at a company but at global commerce? And they utilized the company to stage the attack?

Certainly, someone could have known that, you know, these attacks were targeting major ports, not just in the United States, but globally, shutting down one of the biggest terminals here.

The livelihood of my district is intimately connected with the work that all of you do here, not just in the Port of Los Angeles, but in the Port of Long Beach. It is critically important for me that, you know, you have the support that you need to ensure that you do your job. That is why this bill is so important to me. That is why in last Congress I worked with Buddy Carter to put permanently into law the FLETC program.

I want to ask you about the MLETC program that you have here. So that is, what, a child of the FLETC program? That is, what, an MOU between FLETC and MLETC? Can you explain how that works?

Is that only unique to the Port of Los Angeles Long Beach?

Mr. SEROKA. Yes, it is unique to the Port of Los Angeles where the maritime——

Mrs. TORRES. Exclusively.

Mr. SEROKA [continuing]. Where the Maritime Law Enforcement Center is domiciled here in the Port of Los Angeles, and under the direction of the FLETC, as you had outlined.

One specific statement for the record. We have not predisposed anything with respect to how this or other cyber attacks were first looked at, where they were targeted, who they were going to impact.

We have got to keep a wide line of vision around what we know, what we learn. Putting a lot of that energy, which has also been a constant theme from the committee, as to how we can harness that energy looking forward and evaluating those threats that we don't know of today. How best—and I think the term was just used—how best we can look at what we don't know.

Mrs. TORRES. For example, the unmanned aircraft, the camera systems that are currently watching employees that could be tar-

geted or used as a target to more than watch the employee activities for good or bad. But could, you know, be utilized to do harm.

Mr. SEROKA. Right. It is a daunting task, Congresswoman, because I don't think I would ever in good faith sit here and tell you that we will have everything covered coming out of this meeting.

Our job here as stewards of this agency are to de-risk and minimize risk across a broad cross-section of potential areas of threat.

Looking introspectively at our own vulnerabilities, those which others have cited, and working through that collaborative effort that I mentioned to try to find every way we can to push down——

Mrs. TORRES. My time is very limited. So I am going to have to cut you off there.

Thank you for the effort in creating what you have called a vibrant environment for information sharing. I would love to see how that MLETC model can be implemented at all of our ports, including Ontario Airport, which is very dear and close to me, since I represent that airport.

But also our ports, Oakland, San Diego, and moving on north within California.

To our Coast Guard partners, I want to thank you for all the work that you do.

I was recently in South America and saw some the work that you are doing there in bringing foreign partners to help you see and intercept the narco trafficking that is coming through the Pacific side.

So thank you for your effort.

I understand that you have issues and problems with aging craft. Not just the ships that you have, but other aircraft that you have.

Thank you for doing everything that you are doing with limited resources.

Maybe giving us an appointment to, you know, a Coast Guard academy might help in that.

I yield back, Mr. Chairman.

Chairman MCCAUL. Ranking Member is recognized.

Mr. THOMPSON. Thank you, Mr. Chairman.

I ask unanimous consent to enter into the record a statement from the National Treasury Employees Union.

Chairman MCCAUL. Without objection, so ordered.

[The information referred to follows:]

PREPARED STATEMENT OF ANTHONY M. REARDON, NATIONAL PRESIDENT, NATIONAL TREASURY EMPLOYEES UNION

OCTOBER 30, 2017

Chairman McCaul, Ranking Member Thompson, distinguished Members of the committee, thank you for the opportunity to submit this statement on Customs and Border Protection (CBP) staffing issues on behalf of the 25,000 CBP Officers, Agriculture Specialists and trade enforcement personnel stationed at 328 land, sea, and air ports of entry across the United States (U.S.) and at preclearance stations currently in Ireland, the Caribbean, Canada, and United Arab Emirates airports represented by the National Treasury Employees Union (NTEU).

As of September 2017, CBP's Office of Field Operations (OFO) had 1,200 CBP Officer vacancies. The fiscal year House appropriations bill includes funding to fill the current vacancies to meet the fiscal year CBP Officer on-board target of 24,214, but provides no new funding to address the current CBP Officer staffing shortage of at least 2,500 additional CBP Officers as stipulated by CBP's recently-released Work-

load Staffing Model and to fund an additional 720 CBP Agriculture Specialists as stipulated by CBP most recent Agriculture Resource Allocation Model.

CBP AT THE PORTS OF ENTRY STAFFING SHORTAGE

With the existing vacancy rate of nearly 1,200 funded CBP Officers and, according to CBP's analytic workload staffing model, the need to hire and fund an additional 2,500 CBP Officers to meet fiscal year staffing needs—there is a total CBP Officer staffing shortage of 3,700 today.

The economic cost of this shortage is staggering. For every 33 additional CBP Officers hired, the United States can potentially gain over 1,000 private-sector jobs. If Congress fully staffed the ports with the needed 3,700 additional CBP Officers, 106,000 private-sector jobs could be created. Understaffed ports lead to long delays in travel and cargo lanes and also create a significant hardship for front-line employees. Both involuntary overtime and involuntary work assignments far from home disrupt CBP Officers' family life and destroy morale. Notably, on-going CBP staffing shortages directly contribute to CBP's perennial low ranking in Federal employee workforce satisfaction surveys.

In addition to CBP's trade and travel security, processing and facilitation mission, CBP employees at the ports of entry are the second-largest source of revenue collection for the U.S. Government. In 2016, CBP processed more than $2.2 trillion in imports and collected more than $44 billion in duties, taxes, and other fees.

As you know, the President's January Executive Order calls for hiring 5,000 additional Border Patrol agents and 10,000 new Immigration and Customs Enforcement (ICE) agents, but does not ask for one additional CBP Officer new hire, despite the fact that CBP Officers at the ports of entry in 2016 encountered over 274,000 undocumented immigrants and seized over 600,000 pounds of illegal drugs, and over $62 million in illicit currency, while processing over 390 million travelers and $2.2 trillion in imports through the ports.

CBP STAFFING AT THE PORTS OF LOS ANGELES AND LONG BEACH

The Port of Los Angeles is the No. 1 port by container volume and cargo value in the United States and, along with the Port of Long Beach, is part of the biggest port complex in the United States. NTEU represents approximately 800 CBP front-line employees at the Ports of Los Angeles and Long Beach (LA/LB). In addition to CBP Officers and Agriculture Specialists, these 800 employees also include non-uniformed trade specialists in the LA/LB based Electronics Center for Excellence and Expertise (CEE) along with trade specialists screening incoming commodities represented by all ten CEEs. Since April 2017, the number of front-line employees at LA/LB has been reduced by approximately 45 positions. Staffing shortages at seaports Nation-wide are especially acute. Of the 2,000 CBP Officer new hires funded in fiscal year 2014, fewer than 20, or 1 percent, were assigned to seaports.

The staffing shortage at the CBP San Diego Field Office, that includes the San Ysidro land port, the LA/LB seaport and the Los Angeles International Airport, is indeed critical. In March 2017, there were 350 CBP Officers vacancies at the ports within the San Diego Field Office. Because of the on-going staffing shortages at the Nations' ports, CBP Officers at some ports work up to 16 hours a day and since 2015, CBP OFO has had to divert several hundred CBP Officers from already short-staffed sea, air, and land ports to the critically short-staffed land ports at San Ysidro and Tucson for 90-day stints.

RECOMMENDATIONS

Delays at the U.S. ports of entry result in real losses to the U.S. economy. Understaffed ports lead to long delays in travel and cargo lanes, hurting businesses and consumers, and also create a significant hardship for front-line employees. The 1,200 existing vacancies at U.S. ports of entry must be filled first and 2,500 new CBP Officer and 720 CBP Agriculture Specialists positions need to be funded by Congress.

We ask Congress to reconsider CBP's funding priorities as it finalizes its fiscal year appropriations bills. Unlike other DHS components operating between the ports of entry and at ICE, both of which received significant increases in personnel funding in the fiscal year appropriation bill recently approved by the House, CBP at the ports of entry has established and documented Workload Staffing Models that justify the need to hire 2,500 CBP Officers and 720 Agriculture Specialists today.

If Congress is serious about improving port security, as well as facilitate legal international trade and travel, there is an opportunity to address the justified and documented need to fund additional CBP staffing at the ports in the Omnibus bill that will be considered later this year. On behalf of the men and women represented

by NTEU at the Nation's ports of entry, I urge you to authorize and fund CBP Officers and Agriculture Specialists at least to the levels that Border Patrol and ICE agents are funded in the recently approved fiscal year House appropriations bill.

Thank you for the opportunity to submit this statement to the committee.

Chairman MCCAUL. Let me thank all the witnesses for your testimony. It is very valuable.

I want to thank both the Long Beach and L.A. Port Authority for the tours that we received today.

Want to thank everybody who is attending and for your service day in and day out to protect America's largest port. It is very important to me. That is why I am here.

But as a Texan, I must say, in closing, go Astros.

May not be too popular here.

The committee stands adjourned.

[Whereupon, at 3:06 p.m., the committee was adjourned.]

APPENDIX

LETTER FROM THE NATIONAL ASSOCIATION OF WATERFRONT EMPLOYERS

OCTOBER 24, 2017.

The Honorable MICHAEL MCCAUL,
Chairman, Committee on Homeland Security.

The Honorable BENNIE THOMPSON,
Ranking Minority Member, Committee on Homeland Security.

DEAR CHAIRMAN AND RANKING MEMBER: I am writing on behalf of the National Association of Waterfront Employers (NAWE) to provide comments pertinent to the House Committee on Homeland Security's field hearing on "Examining Physical Security and Cyber Security at our Nation's Ports." NAWE is the voice of marine terminal operators (MTO) and stevedores and has participated in discussions of these issues since the enactment of the Maritime Transportation and Security Act of 2002 and its implementation by the United States Coast Guard (CG). Marine terminal operators buy and operate equipment and hire labor to act as the master link in the global intermodal marine transportation system. The oft characterized importance of the economic contribution by this system cannot be underestimated.

The Department of Homeland Security (DHS) under the Authority of the Congress and the leadership of successive Presidents has orchestrated a system of layered physical security in addressing threats made apparent following 9/11. This layered security includes international port assessments and container inspections by the CG and United States Customs and Border Protection (CBP). It includes advanced notices of arrival and offshore boarding by the CG and CBP. And it includes compliance with CG and CBP regulations by marine terminal operators who form the membership of NAWE. Specifically, it is the marine terminal operator who must have an approved Facility Security Plan (FSP), a designated Facility Security Officer (FSO) and obtain releases for cargo from CBP's Automated Customs Environment (ACE). Recently, NAWE was deeply involved in the planning for a Transportation Workers Identification Card biometric reader and response to the CG's request for comments to its draft Navigation and Vessel Inspection Circular. It is also the MTO that is singularly focused on the success of the business, attending to the diverse objectives of productivity and safety/security. Today's safety/security preserves tomorrow's productivity. NAWE and its members are committed to ensuring that our port's physical and cyber security remain the best in the world.

PHYSICAL SECURITY

Following 9/11, NAWE and it members partnered in the formulation the layered physical security for the global maritime supply chain through the various public forum including local Area Maritime Security Committees. NAWE's members are today a significant investor in and integral component of this system. Efforts in foreign ports and on the high seas/customs waters go relatively unnoticed. However, the continued efforts of the marine terminal operator to be most productive in transferring cargo as the master link in our Nation's cargo chain receive continuous review as necessary to meet their responsibilities under MTSA, the FSP, and the goals of layered security for our ports. The marine terminal operator must evolve and improve while CG and CBP regulations remain constant. The question is whether CG and CBP regulations are able to blend the need for strong security and commercial efficiency.

NAWE applauds the CG's and other agencies current efforts to review its security regulations. However, NAWE seeks continued cooperation with the CG and CBP to develop a unified DHS port security approach including developing a "one-DHS" approach to the FSP and Customer Trade Partnership (CTPAT) as indicators of our collective commitment to the Nation's maritime security. With this much-needed review of regulations and the potential for Congress to act to reauthorize DHS, we

see an opportunity to not only improve security at our Nation's ports, but to also improve on the public-private partnerships that are key to that security. NAWE hopes these actions can result in improved security that works seamlessly with much-needed advancements in commercial efficiencies. If changes to laws and regulations governing our Nation's physical port security are made with input from private-sector partners, NAWE believes both goals can be achieved.

CYBERSECURITY

One need only review the morning news to understand the critical role of strong cybersecurity in our Nation's ports. To understand NAWE commitment to cybersecurity, I refer the committee to NAWE's published response to the CG NVIC 05–17. The NVIC describes the CG interpretation of MTSA to include Cyber requirements throughout the FSP as well as forecasting a "governance" process for the future. Two underlying principles are contained in this response: (1) While MTSA provides clear authority over physical security in protection against kinetic threats, it does not do so over the broad cyber spectrum and (2) NAWE and its members strongly endorse vigorous and vigilant attention to cybersecurity.

First, a few comments on the nature of cyber and cyber systems at port operating facilities. Cyber as something of value is not likely to be the servers and various data terminals, it is likely to be the "information" or "data." Further, the real value is not solely in the information or data, it is in the capability to distribute the information or data within and beyond the facility. It is this distribution capability, especially beyond the facility, which also becomes its vulnerability. This capability is called the World Wide Web—it's the global cyber space.

At port operating facilities you will find the HR, finance, and scheduling capabilities existing at every business of similar size and sophistication around the country. Unique cargo moving systems include load planning, terminal operating systems (TOS), and customs' release authority. Load planning if not on a white board is often done at a centralized location and customs' release is done by the government. The piece of cyber most key to port operations are the TOS. Various terminal operators do not use the same system or even a consistent level of capability. Some operators might be able to function adequately without a technology solution, some could no longer. Higher-end TOS often represents proprietary software and included security measures from the start.

Regarding the record of cyber "incidents," there have been several examples: Releasing cargo (contraband) to the wrong recipient at a European facility, ship-to-shore cranes losing GPS feed, and recently malware which shut down operations at a global operating company. What were the impacts, the causes, the vulnerabilities, and the threats? Was data or cargo compromised? Did they impact the Nation's marine transportation system or even the port-wide system? Are there unifying recovery actions available? What actions, if taken by the Congress or DHS, would have prevented them? These are important questions. MTSA sets out a requirement for assessments such as these questions prior to formulating responsive plans.

As a unifying theme connecting NAWE's first two observations and the following cyber basics, significant public-private partnerships occurred in the development of MTSA physical security in protection from kinetic events. Out of that partnership came the articulation of a "transportation security incident (TSI)." No such discourse or set of definitions exist today with respect to cyber. In fact, NAWE members observe disparate characterizations by the CG of last summer's port cybersecurity event impacting several U.S. port operations. Some have not even recognized that the "event" occurred outside the United States. At a minimum, the Nation and DHS is not prepared to establish policy to provide security from cyber intrusions. Although not able to substantiate its assertion, NAWE believes its members (particularly those most dependent on cargo cyber systems) have as good of understanding of and response to cybersecurity imperatives as the DHS components. NAWE's members are certainly incentivized. This raises the question of whether there is a value-add in governmental well-intended efforts or whether the marketplace is the better incentivizing arena for the port operator's sector. As we develop further technology solutions NAWE members continue to spur better cybersecurity.

NAWE observes recent discussions of the importance of "personal" actions in vulnerabilities and protective measures in cybersecurity. It is interesting that "people" have been raised as more important than technology to cybersecurity at the same time that the full anticipated value of TWIC biometric readers to physical security at marine terminal operations has been reduced.

NAWE's members acknowledge the existence of the NIST framework for cybersecurity. It has value, but is its value in having a lockstep citation within a facility security plan as presented in the recent NVIC or is it a means for the grow-

ing cybersecurity industry to be guaranteed work. NAWE members and their cybersecurity teams go beyond frameworks and look for the best practices to assure protection of their data and business practices from unwanted intrusions. Are best practices an effort that the Congress and DHS can contribute to and how? Is it one that even the disparate terminal operators can gain from working together? These are important questions, yet hard to answer. NAWE is available to continue this discussion.

NAWE members value the CG's protection of SSI information and CBP's efforts to maintain ACE in the face of cyber attacks. Members also value Nationally-accessed information not commercially available which might stimulate the most valuable cybersecurity measures. Like the physical security realm, NAWE members would value National efforts to defeat global criminal and terrorist networks which are the source of many attacks. These efforts might extend to foreign shores but at least should preserve the use of the global cyber space (also known as the World Wide Web) for peaceful and economic purposes as is done for commerce on the high seas. Following events, NAWE members recognize the value of the CG, CBP, and Port Authorities in recovery efforts. These are the kind of efforts DHS (specifically the CG) addressed contemporaneously in developing MTSA and FSP requirements.

NAWE asks that Congress support these efforts of DHS mission focus and most important to the safety and security of our Nation's ports, support the direct involvement of the marine terminal operators in the development, implementation, and execution of port security policies. For NAWE and its members to be effective partners, they need to know that the agencies we work with are empowered to be partners at every step. NAWE members are committed to their contributions to the global marine transportation system, the stimulation of the best productivity possible and the preservation of businesses, jobs, and lives through state-of-the-art safety and security practices.

Sincerely,

JOHN CROWLEY
President, National Association of Waterfront Employers (NAWE).