PROTECTING MARITIME FACILITIES IN THE 21ST CENTURY: ARE OUR NATION'S PORTS AT RISK FOR A CYBER ATTACK?

HEARING

BEFORE THE

SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

OCTOBER 8, 2015

Serial No. 114–35

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

99–577 PDF WASHINGTON : 2016

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
CANDICE S. MILLER, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
JOHN KATKO, New York
WILL HURD, Texas
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BRIAN HIGGINS, New York
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
NORMA J. TORRES, California

BRENDAN P. SHIELDS, *Staff Director*
JOAN V. O'HARA, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

CANDICE S. MILLER, Michigan, *Chairman*

LAMAR SMITH, Texas
MIKE ROGERS, Alabama
JEFF DUNCAN, South Carolina
LOU BARLETTA, Pennsylvania
WILL HURD, Texas
MARTHA MCSALLY, Arizona
MICHAEL T. MCCAUL, Texas *(ex officio)*
FILEMON VELA, Texas
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
BRIAN HIGGINS, New York
NORMA J. TORRES, California
BENNIE G. THOMPSON, Mississippi *(ex officio)*

PAUL L. ANSTINE, *Subcommittee Staff Director*
DEBORAH JORDAN, *Subcommittee Clerk*
ALISON NORTHROP, *Minority Subcommittee Staff Director*

CONTENTS

PROTECTING MARITIME FACILITIES IN THE 21ST CENTURY: ARE OUR NATION'S PORTS AT RISK FOR A CYBER ATTACK?

Thursday, October 8, 2015

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON BORDER AND MARITIME SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 10:02 a.m., in Room 311, Cannon House Office Building, Hon. Candice S. Miller [Chairman of the subcommittee] presiding.

Present: Representatives Miller, Hurd, Vela, Sanchez, and Jackson Lee.

Also present: Representatives Donovan, Ratcliffe, and Langevin.

Mrs. MILLER. In the interest of time, we are expecting a number of other Members, but we are going to start since we have a hard stop today at noon.

The Committee on Homeland Security's Subcommittee on Border and Maritime Security will come to order. The subcommittee is meeting today to examine the cybersecurity efforts at our Nation's ports. We are pleased today to be joined by Admiral Paul Thomas, who is the assistant commandant for prevention policy for the United States Coast Guard; and Mr. Gregory Wilshusen, director of information security issues for the Government Accountability Office; Mr. Randy Parsons, who is director of security services for the Port of Long Beach, California; and Mr. Jonathan Sawicki, who is the security improvement program manager for the Ports of Harlingen and Brownsville, Texas.

We appreciate all of our witnesses coming this morning. I would also at this time ask unanimous consent that the gentleman from New York, Mr. Donovan, a Member of the full committee, be allowed to sit on the dais and participate in today's hearing as well.

Without objection, so ordered.

We appreciate his interest in this subject.

Before we start, I think all of us certainly offer our thoughts and prayers to the family of the 33 crew members of El Faro, which was just a very terrible, tragic event that certainly reminds us all of the force of Mother Nature. But the Coast Guard men and women that went out and performed all the services, the rescues. As it goes forward, we certainly thank all of them for their service all the time, but there it was on vivid display certainly.

The purpose of today's hearing is to examine the vulnerability of seaports to cyber attacks and how well-prepared we are to prevent

and respond to such an attack. Today, this is going to be the first Congressional hearing really convened to examine cybersecurity at our Nation's ports, which I think is fitting since October actually is also National Cybersecurity Awareness Month.

The Coast Guard is the Government agency responsible for the physical security of our Nation's port infrastructures. In working through the Area Maritime Security Committees, the Coast Guard partners with the port authorities and operators to update access controls, fence off sensitive areas of the ports, and increase surveillance, when appropriate, certainly.

Since 9/11, Congress has appropriated $2.4 billion in port security grant funds to harden port facilities against the potential of a terror attack. As a Nation, I think we have done a fairly good job of updating the physical security at the ports, but we certainly have concerns that remain about whether or not the cybersecurity at our ports is adequate. Under the Maritime Transportation Security Act of 2002, the Coast Guard was granted responsibility for the protection of communication systems, including information that flows through the maritime transportation system. Port facilities and ship operators, like many industries in America, are relying certainly increasingly on automation to streamline operations.

While those kinds of innovations certainly reduce time and lower the cost of doing business, they also carry a risk. Terror groups, nation states, criminal organizations, hackers, and even disgruntled employees could breach these systems with potentially catastrophic results to the Nation's economy. More than $1 trillion of goods, from cars to oil to corn and everything in between move through the Nation's seaports each and every year. Increasingly, cargo is moving through our ports using automated industrial control systems. These systems are controlling machinery on ports that move containers or fill tanks and load and offload ships. I understand that the Port of Long Beach and port partners are working toward building, perhaps, the most automated and efficient container terminal in the United States. So we will be looking forward to that testimony from Mr. Parsons about that.

While this automation certainly has a lot of benefits, it doesn't come without risks. In 2014, a major U.S. port facility suffered a system disruption that shut down a significant number of ship-to-shore cranes for several hours. In Europe, drug smugglers attempted to hack into cargo tacking systems to rearrange containers and to hide their drugs. Foreign military is suspected of compromising several systems aboard a commercial ship contracted by the U.S. Transportation Control. These breaches in the maritime domain are certainly concerning not only from an economic standpoint but because of the dangerous cargo, such as liquified natural gas and other certain dangerous cargo that pass through the Nation's seaports. If a cyber breach were to occur that tampered with the industrial control systems that monitor these cargos, it could potentially allow the release of very, very dangerous chemicals.

The private sector, of course, owns the ports and must clearly protect its own interests. However, the Department of Homeland Security has to be involved to ensure communication between ports Nation-wide. Information sharing will undoubtedly be part of any solution that we look to to protect our seaports. We have to have

a strategy that looks beyond individual ports. Just as we have hardened physical security, we need to do the same in the virtual space for systems critical to the maritime transportation system to protect against malicious actors.

The first step in reducing this risk is to conduct risk assessments. The Coast Guard has not yet conducted cyber risk assessments, though some individual ports have taken the initiative themselves. Port security grants can certainly be a way to help port operators make wise choices based on an individual assessment of risk. In providing that grant funding, however, we certainly need to understand which ports are at risk of a cyber incident. Retooling the maritime security risk analysis model to incorporate cyber risks is a concept worth exploring further and incorporating it into the Port Security Grant Program as well.

Then, finally, I think we need to better understand how the Department of Homeland Security, through the National Protection and Programs Directorate and the National Cybersecurity and Communications Integration Center, interfaces with the U.S. Coast Guard's cyber efforts. This is a very technical field, which may or may not be outside of the expertise of the Coast Guard inspector. So despite the exposure for proprietary information, we are wondering whether or not third-party validators, authorized by the Coast Guard, who would have oversight of such a thing, could they review and certify cybersecurity standards. So perhaps there is some merit in looking at that model for cybersecurity. We would be interested in pursuing that as well.

I certainly want to thank the witnesses for appearing before us. I am going to give you a more formal introduction in just a moment.

But the Chair now recognizes our Ranking Member of the subcommittee, the gentleman from Texas, Mr. Vela, for any statement that he may have.

[The statement of Chairman Miller follows:]

STATEMENT OF CHAIRMAN CANDICE S. MILLER

Before we start, I would just like to offer my thoughts and prayers to the family of the 33 crewmembers of the El Faro, the cargo container ship that went missing last week near the Bahamas. I thank the men and women of the Coast Guard for their valiant efforts to find the ship and the missing crew.

The purpose of today's hearing is to examine the vulnerability of seaports to cyber attacks and how well we are prepared to prevent and respond to such an attack.

Our meeting today marks the first Congressional hearing convened to examine cybersecurity at our Nation's ports, which is fitting since October is also National Cybersecurity Awareness Month.

The United States Coast Guard is the Government agency responsible for the physical security of our Nation's port infrastructure. Working through the Area Maritime Security Committees, the Coast Guard partners with port authorities and operators to update access controls, fence-off sensitive areas of the ports, and increase surveillance when appropriate.

Since the terrorist attacks of September 11, 2001, the United States Congress has appropriated $2.4 billion dollars in port security grant funds to harden port facilities against the potential for a terror attack. As a Nation, we have done a fairly good job updating the physical security at ports, but I am concerned that the U.S. Government has fallen behind when it comes to the cybersecurity of the port.

Under the Maritime Transportation Security Act of 2002, the U.S. Coast Guard was granted responsibility for the protection of communication systems, including information that flows through the Marine Transportation System. Port facilities and ship operators, like many industries in America, increasingly rely on automa-

tion to streamline operations. While those innovations reduce the time it takes to stock our shelves, and lower the cost of doing business, they also carry risk.

Terror groups, nation-states, criminal organizations, hackers and even disgruntled employees could breach these systems—with potentially catastrophic results to the Nation's economy.

More than $1 trillion dollars of goods, from cars to oil to corn and everything in between move through the Nation's seaports every year.

Increasingly, cargo is moving through our ports using automated industrial control systems. These computer systems are controlling machinery on ports to move containers, fill tanks and on-load and off-load ships.

I understand that the Port of Long Beach and port partners are working towards building perhaps the most automated and efficient container terminal in the United States. Once completed it will reduce wait times at the ports and increase throughput.

While this automation has substantial benefits, it does not come without risks. In 2014, a major U.S. port facility suffered a system disruption that shut down a significant number of ship-to-shore cranes for several hours. In Europe, drug smugglers attempted to hack into cargo tracking systems to rearrange containers and hide their drugs. Similarly, a foreign military is suspected of compromising several systems aboard a commercial ship contracted by the U.S. Transportation Command.

These breaches in the maritime domain are particularly concerning, not only from an economic standpoint, but because of the dangerous cargo such as Liquefied Natural Gas, and other Certain Dangerous Cargos that also pass through the Nation's seaports. If a cyber breach were to occur that tampered with the industrial control systems that monitor these cargos, it could potentially allow the release of harmful and dangerous chemicals.

Despite the fact the GAO has placed cyber security of our Nation's critical infrastructure on the "High Risk" list since 2003, the Coast Guard, and DHS as a whole, have been slow to fully engage on cybersecurity efforts at the Nation's 360 seaports.

The threat of cyber attack is worrisome to be sure. But when it comes to the maritime domain and the protection of maritime critical infrastructure, who is really in charge?

The private sector owns the ports, and must clearly protect its own interests. However, the Department of Homeland Security must be involved to ensure communication between ports Nation-wide. Information sharing will undoubtedly be part of any solution as we look to protect our seaports and we must have a strategy that looks beyond individual ports.

Just as we have hardened physical security, we need to do the same in the virtual space for systems critical to the marine transportation system to protect against malicious actors. The first step in reducing this risk is to conduct risk assessments. The Coast Guard has not yet conducted cyber risk assessments, though some individual ports have taken the initiative themselves.

Port security grants can be a way to help port operators make wise choices based on an individual assessment of risk. In providing grant funding, however, we must understand which ports are at risk of a cyber incident. Retooling the Maritime Security Risk Analysis Model to incorporate cyber risks is a concept worth exploring further and incorporating into the port security grant program.

Finally, I want to better understand how DHS, through the National Protection and Programs Directorate (NPPD) and the National Cybersecurity and Communication Integration Center, interfaces with the U.S. Coast Guard's cyber efforts.

We are all aware that the Government moves slowly and this can cause us to quickly fall behind, especially in an area like cyber that moves rapidly.

With that in mind, should the Coast Guard's role in cyber be limited to oversight and prevention rather than the creation of standards?

This is a very technical field which may be outside the expertise of a Coast Guard Inspector. Therefore, despite the exposure to proprietary information, could third-party validators, authorized by the Coast Guard, review and certify cybersecurity standards? I think there is merit in looking at that model for cybersecurity and would be interested in hearing from the witnesses on that topic.

I thank the witnesses for appearing before us today and look forward to their testimony.

Mr. VELA. Chairman Miller, thank you for holding today's hearing to discuss the threat of cyber attack at ports and what the U.S. Coast Guard and the Department of Homeland Security are doing with private and public partners to protect maritime critical infra-

structure against such attacks. I thank all our witnesses for being with us here today.

Since the Coast Guard is responsible for the security of our Nation's ports, entities both in the private sector and in local and State government rely on the service's leadership when doing their part to mitigate risks at our ports. As Ranking Member of the subcommittee and as a Member representing a district along the Gulf of Mexico, I have an interest in port security issues and recognize the unique challenges each port faces.

Texas' District 34 includes four maritime ports—the Port of Brownsville, the Port of Harlingen, Port Isabel, and Port Mansfield—and is adjacent to the Port of Corpus Christi, which is represented by Congressman Farenthold. Each of these ports has its own set of characteristics, managing various volumes and types of cargo and other commercial traffic. One of the differences is, for example, the Port of Brownsville and the Port of Harlingen are about 17 miles inland whereas the port of Corpus Christi is right adjacent to a city of 300,000 people. I have met with the chief of police at the Port of Corpus Christi. I know he has some concerns about some of the vulnerabilities there. I look forward to hearing about that. As with other ports, facilitating the flow of commerce must be judiciously balanced with measures required to keep our ports secure. As in my district, many of our Nation's ports are closely linked to other vital transportation networks and critical infrastructure which often lead to major metropolitan areas.

Traditionally, our focus has been on the physical security of these ports. Today, we will discuss an important element that is growing and rapidly evolving, the use of technology at ports and the security risks posed by our increased reliance on these automated and networked systems. There is no question that technology can enhance the operations and security of seaports which, in turn, helps boost economies through the import and export of goods. This technology also adds an additional level of risk that we must better understand and mitigate.

Though this subcommittee does not typically discuss cybersecurity, it is important that we understand the Federal Government's role in this important port security issue. Last June, the Government Accountability Office issued a report on cybersecurity at ports. Its findings highlighted several actions the Coast Guard and DHS as a whole should take in order to better prepare for and ideally prevent cyber attacks on systems used at seaports. In June, the Coast Guard published their cyber strategy, which discussed the need to include cybersecurity as an element of security regimes for maritime critical infrastructure. Today, I hope to better understand how the GAO's findings influenced Coast Guard cyber strategy and how it will help inform implementation of the strategy.

I would like to learn more about how the Coast Guard is developing guidance and standards that will address safety and security concerns while being sufficiently flexible for ports around the country. There are no one-size-fits-all solutions. What works in Long Beach may well not work best for Brownsville, for example. I also hope to hear directly from our port witnesses today about how ports of different types and sizes are addressing cybersecurity and

what more the Coast Guard, DHS, and Congress can do to support your efforts.

I am hopeful that today's hearing will broaden the subcommittee's understanding of the emerging risks related to technology at our ports.

With that, Madam Chairman, I yield back the balance of my time.

Mrs. MILLER. I thank the gentleman very much. Members are reminded that additional statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

OCTOBER 8, 2015

The Committee on Homeland Security has long been engaged on the issues of cybersecurity, port security, and critical infrastructure protection. This hearing brings those critical issues together by focusing on cybersecurity at America's ports.

A 2014 Government Accountability Office (GAO) report found that actions taken by the Department of Homeland Security (DHS) and other Federal agencies to address cybersecurity in the maritime port environment have been limited. So much of the focus has been on improving the physical security at ports that cybersecurity at ports, an emerging threat, has been secondary.

In recent years, cyber technology has helped promote efficient port operations and enhanced security. But these benefits come with risks to the Maritime Transportation System. For example, in 2013, officials at Europol disclosed that a group of drug traffickers recruited hackers to breach information technology systems at the Port of Antwerp to smuggle container loads of cocaine.

Our cargo security programs are predicated on electronic transmission of manifest data, underscoring the potential risk of such cyber breaches not just from drug smugglers, but also other criminals and even terrorists. Requiring the Coast Guard to complete a cyber risk assessment and ensure that cyber risks are addressed in maritime security plans, as recommended by GAO, is a good first step toward reducing cyber vulnerabilities at ports.

Similarly, allowing Port Security Grant Program funds to be used for cybersecurity, and ensuring the funds are used effectively, is a step in the right direction. The Coast Guard's June 2015 Cyber Strategy presents cyber space as another operational domain for the Service, and sets forth three strategic priorities: Defending cyber space, enabling operations, and protecting infrastructure.

I look forward to hearing from the Coast Guard today about how they intend to implement this Strategy, with the help of other Government and private-sector stakeholders. I also want to hear from GAO about what more can be done by DHS and the Coast Guard in this domain, as Coast Guard implements its strategy.

Finally, I want to discuss with the ports how we can support their cybersecurity efforts, recognizing that each port is different and no single solution is likely to be appropriate for all. Certainly, providing ports and other stakeholders, like terminal operators and transportation companies, with the appropriate guidance and expertise will be essential. Adequate resources are also going to be necessary to address cybersecurity risks at ports, and Congress must provide those resources and help ensure they are used wisely.

Mrs. MILLER. Again, we are pleased to be joined by four very distinguished witnesses today to discuss this very important topic. In way of a more formal introduction, Rear Admiral Paul Thomas serves as the assistant commandant for prevention policy in the United States Coast Guard. In this role, Admiral Thomas oversees three Coast Guard directorates: Inspections and Compliance; Marine Transportation Systems; and Commercial Regulations and Standards. In addition to his assignment at the Coast Guard headquarters here in Washington, Admiral Thomas has also served in San Francisco, Port Canaveral, Florida, and Galveston, Texas.

Mr. Gregory Wilshusen is the director of information security issues at GAO, where he leads cybersecurity and privacy-related studies and audits of the Federal Government and critical infrastructure. He has over 30 years of auditing, financial management, and information systems experience, having served at the Department of Education before joining the GAO in 1997.

Mr. Randy Parsons is the director of security services for the Port of Long Beach, California, the Nation's second-busiest seaport, a position that he has held since the fall of 2012. Mr. Parsons oversees more than 80 security personnel, including harbor patrol officers. He directs the homeland security program for the 3,000-acre port complex, including 24-hour patrol, antiterrorism programs, and security coverage. He has a long history of public service, which includes time with the FBI and at TSA. Mr. Jonathan Sawicki is the security improvement program manager for the Ports of Brownsville and Harlingen, Texas, where since 2008, he has assisted in the development of port-wide security strategic risk management plans, including a TWIC card reader deployment program at the Port of Brownsville.

So their full written statements will appear in the record.

The Chair now recognizes Admiral Thomas for his testimony. Thank you, sir.

STATEMENT OF REAR ADMIRAL PAUL F. THOMAS, ASSISTANT COMMANDANT, PREVENTION POLICY, U.S. COAST GUARD, U.S. DEPARTMENT OF HOMELAND SECURITY

Admiral THOMAS. Thank you, Madam Chairman. Good morning. Good morning to the distinguished Members of the committee. Thank you for your continued strong support of the Coast Guard and for this opportunity to talk about the very important, relevant, and timely topic of cyber in the maritime sector.

Madam Chairman, if I may, before we begin this morning, join you in offering, on behalf of all the men and women of the Coast Guard, our deepest condolences to the families of the 33 souls that were lost aboard El Faro last week. As mariners and maritime professionals, we know only too well the perils that all those who serve our Nation at sea face. We felt the loss of El Faro very deeply.

Madam Chairman, as has already been mentioned, the Coast Guard recently released our cyber strategy. That strategy recognizes that cyber does not represent a new mission for the Coast Guard but is, in fact, a domain in which we must be able to operate effectively in order to conduct all of our missions, including our response and our prevention missions. In that sense, the Coast Guard authorities, responsibilities, roles, and missions naturally extend into cyber space. The cyber strategy identifies three priorities for our service: Defending our own cyber space, enabling Coast Guard operations, and protecting critical maritime infrastructure.

It is this third priority that falls within my purview and the Coast Guard and which I understand is of most interest to this committee today. The Coast Guard is really well-suited to take a leadership role in addressing cyber risks to maritime critical infrastructure as part of the larger interagency effort led by the Department of Homeland Security and in conjunction with maritime

stakeholders. The Coast Guard, as has already been mentioned, has a long history of working with port partners across the interagency to mitigate safety, security, and environmental risks to U.S. ports. We will take the same approach in the cyber domain. The Coast Guard is the sector-specific agency for maritime transportation under the National Infrastructure Protection Plan. Whether the initiating event occurs in cyber space or in a physical domain, the Coast Guard already has broad authority and responsibility under the Maritime Transportation Security Act to prevent transportation security incidents. We have similar authority and responsibility under a number of statutes to prevent accidents and incidents that may damage people, property, or the environment. We have an existing regulatory structure that requires regulated industry to assess safety, security, and environmental risks, and to address those risks.

The Coast Guard has already undertaken significant effort within the interagency, industry, academia, and with our international partners to assess and understand cyber risk in a maritime transportation system. In the course of this work, we have leveraged the expertise that exists at the Department of Homeland Security, the Department of Energy, the Department of Defense, the National Institute for Standards and Technology to many others. Our ultimate goal is to incorporate cyber risk management into the existing safety and security regimes that have served the maritime industry and the American public so well for so long. Of course, in doing so, we will remain focused, as we always have, on risk-based performance standards that provide flexible, layered protection against cyber risks while allowing the benefits of cyber-enabled operations in the MTS.

There is no doubt, it has been mentioned, cyber capabilities that make our transportation systems more effective, efficient, productive, and environmentally friendly also introduce operational risks that now have to be managed effectively. We have already seen incidents in the maritime transportation system that have resulted in physical consequences or significant near misses. In some cases, it would appear that these were intentional actions, perhaps by actors with malicious intent. But in other cases, they were clearly accidents caused by improper use or maintenance of cyber systems. That is why cyber is both a safety and a security issue. That is why the Coast Guard is holistically addressing cyber risk management as just that, a risk management challenge. Thank you for your time and attention. I look forward to hearing from the rest of the panelists and to further discussion.

[The prepared statement of Admiral Thomas follows:]

PREPARED STATEMENT OF PAUL F. THOMAS

OCTOBER 8, 2015

INTRODUCTION

Good morning Madam Chairman and distinguished Members of the committee. I am honored to be here to discuss cybersecurity in U.S. ports. I will focus my comments in three areas. The first is to recognize the importance of cybersecurity and then explain cyber safety concerns, which emphasize the need to view this issue as a "cyber risk management" challenge. The second is to explain the need for an ap-

proach that emphasizes the essential role and responsibilities of maritime industry partners. The third is to outline what we have achieved and propose a way forward.

The Coast Guard has a long history of working with port partners to mitigate safety, security, and environmental risks to U.S. ports and maritime critical infrastructure. Since our founding in 1790, we have patrolled in 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 to execute these authorities and work with our partners to prepare our ports for natural disasters, accidents, and deliberate acts.

Over time, the Coast Guard and the maritime industry have cooperated 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 cargos to containerization, with sophisticated systems now controlling the movement and tracking of containerized and liquid cargos.

The Coast Guard's recently-developed Cyber Strategy proposes three strategic priorities for the service—defending our own cyber space, enabling Coast Guard operations, and protecting maritime critical infrastructure. Cybersecurity in U.S. ports is a key goal of this strategy.

CYBER RISKS AND THE MARINE TRANSPORTATION SYSTEM

Similar to other sectors, emerging cyber threats in the port environment are diverse and complex. Cyber risks manifest themselves as both safety and security concerns. As such, the Coast Guard is emphasizing the term "cyber risk management," which also addresses how much the maritime transportation system (MTS) relies on information technology systems to connect to the global supply chain. Vessel and facility operators use computers and cyber-dependent systems for navigation, communications, engineering, cargo, ballast, safety, environmental control, and emergency systems such as security monitoring, fire detection, and alarm systems. Collectively these systems enable the MTS to operate with an impressive record of efficiency and reliability.

While these information technology systems create benefits, they also introduce potential risks. Exploitation, misuse, or simple failure of information technology systems can cause injury or death, harm the marine environment, or disrupt vital trade activity.

Outside the United States, cyber-related incidents among technology systems have been reported ranging from container terminal operations ashore to offshore platform stability and dynamic positioning for offshore supply vessels. While in some cases criminals may have been the source of these events, others have been the result of non-targeted malware or relatively unsophisticated insider threats. Even legitimate functions, such as remotely-driven software updates, can disable vital systems if done at the wrong time or under the wrong conditions.

In one well-publicized event, organized crime exploited a European container terminal's cargo tracking system to facilitate drug smuggling. Cargo control is also one of the requirements of the Coast Guard's Maritime Transportation Security Act (MTSA) regulations, and we are well aware that such an incident, or one even more serious, might occur in the United States.

"Cyber risk management" also has safety implications. We are aware of incidents in which software problems led to the failure of dynamic positioning or navigation systems. These were not due to targeted attacks, but malware that migrated to vital systems through poor information technology practices.

As port facilities and vessels continue to incorporate information technology systems into their operations, the Coast Guard must adapt its regulatory regime accordingly. Regardless of whether an incident is a cyber attack, or a cyber accident, we must recognize the potential consequences to mariners, port workers, the public, and the marine environment. With approximately 360 sea and river ports that handle more than $1.3 trillion in annual cargo, our Nation is critically dependent on a safe, secure, and efficient MTS.

UNITY OF EFFORT—PARTNERSHIPS, LEARNING, AND COORDINATION

The Coast Guard is working closely with the Department of Homeland Security (DHS) and other Government agencies to help the maritime industry identify their cyber risks.

This past March, the Coast Guard sponsored a seminar at the DHS Center of Excellence at Rutgers University on maritime cyber risks. We held a similar event at the Coast Guard Academy, and a follow-up at the California Maritime Academy to address specific cyber research questions. Each of these events included a broad range of cyber practitioners from industry, Government, and academia.

In another effort, the Coast Guard Research and Development Center (supported by DHS S&T/Cyber Security Division) recently evaluated cyber vulnerabilities associated with wireless access to maritime critical infrastructure at certain U.S. ports. The preliminary results indicate significant vulnerabilities. While this study is relatively narrow in scope, the Coast Guard is continuing to evaluate the broad range of cyber risks in the maritime domain.

The Coast Guard has also partnered with various groups to evaluate and address cyber risks more systematically. Working with the American Association of Port Authorities and the National Institute of Standards and Technology (NIST), we are developing a cyber risk profile for bulk liquid terminals—such as those that transfer oil, gasoline, and liquid hazardous materials.

Another area with potentially significant consequences is the offshore oil and natural gas industry. This industry relies on information technology systems for a wide variety of functions—from the dynamic positioning systems that allow for precise navigation control, even in heavy wind and sea conditions, to real-time monitoring of drilling and production activity. Along with senior representatives from industry, the Department of Energy, and DHS, I recently attended a meeting of the Energy Sector Coordinating Committee in Houston. The exclusive purpose of this meeting was to discuss cyber risks. While the potential threats to this industry could be serious, I was very pleased with the cooperation and realistic approach that the participants expressed. As part of a related effort, the Coast Guard is working with the National Offshore Safety Advisory Committee to address cyber risks in the offshore industry.

Our work with other agencies, advisory bodies, and institutions has helped us identify the standards and best practices that can reduce risk. The Coast Guard is a strong advocate for using effective cybersecurity tools, guidelines, and sources of information. These include the Cybersecurity Framework developed by the NIST, the Cyber Capability Maturity Model developed by the Department of Energy, and the services provided by DHS's Computer Emergency Response Team (CERT), among others.

INTERNATIONAL CONSIDERATIONS

Cyber risks are an inherently global issue, and cooperation with international partners is an important part of our strategy. Covert electronic surveillance by foreign ships visiting our ports is a long-standing security concern, and cyber technology certainly provides new avenues for such activity. Sound cyber practices by marine terminals can help minimize the likelihood that they might become victims of such activity, or of less nefarious activity that might still impact their business or operations.

Failure to follow sound cyber practices may create as much risk as not conducting proper equipment maintenance or adequate crew training for conventional shipboard emergencies. Accordingly, the Coast Guard is working within the International Maritime Organization to incorporate cyber risks into Safety Management System requirements, as well as the International Ship and Port Facility Security (ISPS) Code. While this is a deliberate and lengthy process, we have strong support from several nations, including Canada, South Korea, and Japan.

COAST GUARD ACTIVITIES TO ADDRESS CYBER RISKS IN THE MARINE TRANSPORTATION SYSTEM

The Coast Guard is and has been working to address cyber risks in the Marine Transportation System. In 2012, we directed all of our Area Maritime Security Committees (AMSC) to consider cyber issues alongside more conventional risks as they evaluated potential security risks to their ports. Required by the MTSA, AMSCs are public-private partnerships that are chaired by the local Captain of the Port. All port stakeholders are represented at their local AMSC, including representatives from the Federal, State, and local government, as well as private industry and labor.

Across the country, AMSCs have established cyber subcommittees, evaluated cybersecurity risks, held cyber-related exercises, and assisted in the evaluation of port security grant funding, including grants directed specifically at cybersecurity vulnerabilities. AMSCs also serve as a forum to share best practices across Government and industry, such as the FBI's InfraGard program.

Because no amount of effort can guarantee that a cyber incident will not occur, the management of cyber risk demands a significant resilience and recovery aspect. AMSCs include a recovery annex to their Area Maritime Security Plans and these annexes are well-suited to include cyber events as an element in port contingency planning. If or when there is a cyber incident in any given port area, our collective goal must be to continue safe and secure operations with minimal disruptions.

CURRENT CHALLENGES AND FUTURE PLANS

The Coast Guard has made considerable progress in improving our own understanding of cyber risks, as well as improving cyber preparedness in ports and across the maritime industry. Despite these accomplishments, we know that significant work remains.

Our ultimate goal is to incorporate cyber risk management into the existing safety and security regimes that have served the industry, the Coast Guard, and the public so well, for so long. This past January, we held a public meeting to solicit suggestions on how to best accomplish this goal. We will continue to engage with industry and the public as we proceed.

The complexity of cyber technology, and the fast pace of change, suggest that any requirements will need to be risk- and performance-based. That is, rather than mandate a specific technical solution, the Coast Guard believes that facility and vessel operators should identify and evaluate the vulnerabilities and consequences associated with their cyber systems, and put in place an appropriate suite of mitigating measures sufficient to achieve an acceptable level of security. This approach has served the industry and public well in conventional safety and security risks. Our challenge is to devise a methodology suited to the nuances of cyber risk. Of course it must produce meaningful results in a way that the vessel or facility operators can demonstrate an acceptable level of security to the Coast Guard and other interested parties.

In addition to policy development, we recognize the need to develop our own workforce and take other measures to ensure we have the capacity and skills necessary to carry out those policies. The Coast Guard Cyber Strategy identifies several factors to this end, including training, education, organizational structure, and partnerships.

In addressing cyber risks to ports and other aspects of the maritime industry, our commitment is to address those risks with the same level of professionalism, efficiency, and effectiveness that the public has come to expect. The Coast Guard will continue to adapt, as it has done over the last two centuries, to the challenges and opportunities that accompany technological advancements in our operating environment.

Thank you for the opportunity to testify today, and thank you for your continued support of the United States Coast Guard. I am pleased to answer your questions.

Mrs. MILLER. Thank you very much.

The Chair now recognizes Mr. Wilshusen for his testimony.

STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Miller, Ranking Member Vela, and Members of the subcommittee, thank you for inviting me to testify today at today's hearing on cybersecurity risks facing our Nation's maritime facilities.

As you know, maritime ports are an essential part of the United States transportation critical infrastructure and handle more than $1.3 trillion of cargo each year. A major disruption in the maritime transportation system could have a significant impact on global shipping, international trade, and our National economy.

Today I will summarize GAO's report on maritime port cybersecurity that we issued back in June 2014. The report addresses cyber-related threats facing our Nation's ports and the steps the U.S. Coast Guard and other stakeholders had taken to address cyber risks. But before I began, Madam Chairman, if I may, I would like to recognize several teammates who were instrumental

in developing my statement and conducting the work underpinning it. Mike Gilmore, who is with me today, is an assistant director and led this engagement; along with Brad Becker; and Kush Malhotra. Lee McCracken, Jennifer Bryant, and Scott Pettis also made significant contributions to this effort.

Madam Chairman, our Nation and its ports face an evolving array of cyber-based threats. The increasing dependence of port activities on computerized information and communication systems to manage the movement of cargo makes them vulnerable to many of the same threats facing other cyber-reliant critical infrastructure. These threats include both targeted and untargeted exploits from a variety of sources, including criminal groups, nation-states, and state-sponsored entities, and disgruntled insiders. By exploiting vulnerabilities in information and communication technology supporting port operations, cyber adversaries can potentially disrupt the flow of commerce, endanger public safety, and facilitate the theft of valuable cargo.

In June 2014, we reported that the Coast Guard and other stakeholders had taken limited steps to address cybersecurity at selected ports. Specifically, the Coast Guard had not included cyber-related risks in its 2012 biannual assessment of risk to the maritime environment. Maritime security plans required by law and regulation generally contained very limited information on cyber threats and vulnerabilities because the guidance issued by the Coast Guard did not require cyber elements to be addressed.

In addition, the Coast Guard helped to establish information-sharing mechanisms. But one of them, a maritime sector coordinating council comprised of private-sector stakeholders, disbanded in 2011, eliminating a National-level forum for sharing and coordinating information on port security. We also reported that the Federal Emergency Management Agency, or FEMA, identified enhancing cybersecurity capabilities as a priority for its Port Security Grant program. However, its grant review process was not informed by Coast Guard cybersecurity expertise, thereby increasing the risks that the grants were not allocated to projects that would effectively enhance port security.

In our 2014 report, we recommended that the Coast Guard include cyber risks in its updated risk assessment for the maritime environment, address cyber risks in its guidance for maritime security plans, and consider reestablishing the sector coordinating council. We also recommended that FEMA ensure funding decisions for its Port Security Grant Program are informed by cybersecurity expertise and a comprehensive risk assessment.

DHS concurred with our recommendations. Since our report was issued in 2014, the Coast Guard and FEMA have taken actions to partially implement two of our recommendations. In summary, protecting our maritime ports from cyber-based threats is of increasing importance. While the Coast Guard and FEMA have taken steps, more needs to be done to ensure that the Federal and non-Federal stakeholders are working together effectively to mitigate these threats. Fully implementing our recommendations will help the Coast Guard and FEMA achieve this.

Chairman Miller, Ranking Member Vela, and Members of this committee, this concludes my opening statement. I would be happy to answer your questions.

[The prepared statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN

OCTOBER 8, 2015

GAO HIGHLIGHTS

Highlights of GAO–16–116T, a testimony before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

The Nation's maritime ports handle more than $1.3 trillion in cargo each year: A disruption at one of these ports could have a significant economic impact. Increasingly, port operations rely on computerized information and communications technologies, which can be vulnerable to cyber-based attacks. Federal entities, including DHS's Coast Guard and FEMA, have responsibilities for protecting ports against cyber-related threats. GAO has designated the protection of Federal information systems as a Government-wide high-risk area since 1997, and in 2003 expanded this to include systems supporting the Nation's critical infrastructure.

This statement addresses: (1) Cyber-related threats facing the maritime port environment and (2) steps DHS has taken to address cybersecurity in that environment. In preparing this statement, GAO relied on work supporting its June 2014 report on cybersecurity at ports. (GAO–14–459)

What GAO Recommends

In its June 2014 report on port cybersecurity, GAO recommended that the Coast Guard include cyber risks in its updated risk assessment for the maritime environment, address cyber risks in its guidance for port security plans, and consider reestablishing the sector coordinating council. GAO also recommended that FEMA ensure funding decisions for its port security grant program are informed by subject-matter expertise and a comprehensive risk assessment. DHS has partially addressed two of these recommendations since GAO's report was issued.

MARITIME CRITICAL INFRASTRUCTURE PROTECTION.—DHS NEEDS TO ENHANCE EFFORTS TO ADDRESS PORT CYBERSECURITY

What GAO Found

Similar to other critical infrastructures, the Nation's ports face an evolving array of cyber-based threats. These can come from insiders, criminals, terrorists, or other hostile sources and may employ a variety of techniques or exploits, such as denial-of-service attacks and malicious software. By exploiting vulnerabilities in information and communications technologies supporting port operations, cyber attacks can potentially disrupt the flow of commerce, endanger public safety, and facilitate the theft of valuable cargo.

In its June 2014 report, GAO determined that the Department of Homeland Security (DHS) and other stakeholders had taken limited steps to address cybersecurity in the maritime environment. Specifically:

- DHS's Coast Guard had not included cyber-related risks in its biennial assessment of risks to the maritime environment, as called for by Federal policy. Specifically, the inputs into the 2012 risk assessment did not include cyber-related threats and vulnerabilities. Officials stated that they planned to address this gap in the 2014 revision of the assessment. However, when GAO recently reviewed the updated risk assessment, it noted that the assessments did not identify vulnerabilities of cyber-related assets, although it identified some cyber threats and their potential impacts.
- The Coast Guard also did not address cyber-related risks in its guidance for developing port area and port facility security plans. As a result, port and facility security plans that GAO reviewed generally did not include cyber threats or vulnerabilities. While Coast Guard officials noted that they planned to update the security plan guidance to include cyber-related elements, without a comprehensive risk assessment for the maritime environment, the plans may not address all relevant cyber threats and vulnerabilities.
- The Coast Guard had helped to establish information-sharing mechanisms called for by Federal policy, including a sector coordinating council, made up of

private-sector stakeholders, and a Government coordinating council, with representation from relevant Federal agencies. However, these bodies shared cybersecurity-related information to a limited extent, and the sector coordinating council was disbanded in 2011. Thus, maritime stakeholders lacked a National-level forum for information sharing and coordination.

- DHS's Federal Emergency Management Agency (FEMA) identified enhancing cybersecurity capabilities as a priority for its port security grant program, which is to defray the costs of implementing security measures. However, FEMA's grant review process was not informed by Coast Guard cybersecurity subject-matter expertise or a comprehensive assessment of cyber-related risks for the port environment. Consequently, there was an increased risk that grants were not allocated to projects that would most effectively enhance security at the Nation's ports.

GAO concluded that until DHS and other stakeholders take additional steps to address cybersecurity in the maritime environment—particularly by conducting a comprehensive risk assessment that includes cyber threats, vulnerabilities, and potential impacts—their efforts to help secure the maritime environment may be hindered. This in turn could increase the risk of a cyber-based disruption with potentially serious consequences.

Chairman Miller, Ranking Member Vela, and Members of the Subcommittee: Thank you for inviting me to testify at today's hearing on the risks of cyber attacks facing our Nation's maritime facilities. As you know, maritime ports are an essential part of the United States' transportation critical infrastructure. They are an economic engine that handles more than $1.3 trillion in cargo each year. A major disruption in the maritime transportation system could have a significant impact on global shipping, international trade, and the global economy, as well as posing risks to public safety. This risk is heightened by ports' dependence on computer-reliant information and communication systems that may be vulnerable to cyber threats from various actors with malicious intent. Because of the increasing prevalence of cyber threats, since 1997 we have designated Federal information security as a Government-wide high-risk area, and in 2003 we expanded this to include the protection of systems supporting our Nation's critical infrastructure.[1]

In my statement today, I will summarize the results of a report we issued in June 2014 on the extent to which the Department of Homeland Security (DHS) and other stakeholders have addressed cybersecurity in the maritime port environment.[2] Specifically, I will discuss: (1) Cyber-related threats facing the maritime port environment and (2) steps DHS and other stakeholders have taken to address cyber risks in the maritime environment, as well as provide updates on actions DHS has taken to implement recommendations we made in our report. More detailed information on our objective, scope, and methodology for that work can be found in the issued report.

The work on which this testimony is based was conducted in accordance with generally-accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

The United States has approximately 360 commercial sea and river ports that handle more than $1.3 trillion in cargo annually. A wide variety of goods travels through these ports each day—including automobiles, grain, and millions of cargo containers. While no two ports are exactly alike, many share certain characteristics such as their size, proximity to a metropolitan area, the volume of cargo they process, and connections to complex transportation networks. These characteristics can make them vulnerable to physical security threats.

Moreover, entities within the maritime port environment are vulnerable to cyber-based threats because they rely on various types of information and communications technologies to manage the movement of cargo throughout the ports. These technologies include:

---

[1] GAO's biennial high-risk list identifies Government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need to address challenges to economy, efficiency, or effectiveness. See most recently, GAO, *High-Risk Series: An Update,* GAO–15–290 (Washington, DC: Feb. 11, 2015).

[2] GAO, *Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity,* GAO–14–459 (Washington, DC: June 5, 2014).

- terminal operating systems, which are information systems used to, among other things, control container movements and storage;
- industrial control systems, which facilitate the movement of goods using conveyor belts or pipelines to structures such as refineries, processing plants, and storage tanks;
- business operations systems, such as e-mail and file servers, enterprise resources planning systems, networking equipment, phones, and fax machines, which support the business operations of the terminal; and
- access control and monitoring systems, such as camera surveillance systems and electronically-enabled physical access control devices, which support a port's physical security and protect sensitive areas.

All of these systems are potentially vulnerable to cyber-based attacks and other threats, which could disrupt operations at a port.

Federal Policies and Laws Establish Requirements and Responsibilities for Protecting Maritime Critical Infrastructure

While port owners and operators are responsible for the cybersecurity of their operations, Federal agencies have specific roles and responsibilities for supporting these efforts. The National Infrastructure Protection Plan (NIPP) establishes a risk management framework to address the risks posed by cyber, human, and physical elements of critical infrastructure. It details the roles and responsibilities of DHS in protecting the Nation's critical infrastructures; identifies agencies that have lead responsibility for coordinating with Federally-designated critical infrastructure sectors (maritime is a component of one of these sectors—the transportation sector); and specifies how other Federal, State, regional, local, Tribal, territorial, and private-sector stakeholders should use risk-management principles to prioritize protection activities within and across sectors.

The NIPP establishes a framework for operating and sharing information across and between Federal and non-Federal stakeholders within each sector. These coordination activities are carried out through sector-coordinating councils and Government-coordinating councils. Further, under the NIPP, each critical infrastructure sector is to develop a sector-specific plan that details the application of the NIPP risk management framework to the sector. As the sector-specific agency for the maritime mode of the transportation sector, the Coast Guard is to coordinate protective programs and resilience strategies for the maritime environment.

Further, Executive Order 13636, issued in February 2013, calls for various actions to improve the cybersecurity of critical infrastructure.[3] These include developing a cybersecurity framework; increasing the volume, timeliness, and quality of cyber threat information shared with the U.S. private sector; considering prioritized actions within each sector to promote cybersecurity; and identifying critical infrastructure for which a cyber incident could have a catastrophic impact.

More recently, the Cybersecurity Enhancement Act of 2014[4] further refined public-private collaboration on critical infrastructure cybersecurity by authorizing the National Institute of Standards and Technology to facilitate and support the development of a voluntary set of standards, guidelines, methodologies, and procedures to cost-effectively reduce cyber risks to critical infrastructure.

In addition to these cyber-related policies and law, there are laws and regulations governing maritime security. One of the primary laws is the Maritime Transportation Security Act of 2002 (MTSA)[5] which, along with its implementing regulations developed by the Coast Guard, requires a wide range of security improvements for the Nation's ports, waterways, and coastal areas. DHS is the lead agency for implementing the act's provisions, and DHS component agencies, including the Coast Guard and the Federal Emergency Management Agency (FEMA), have specific responsibilities for implementing the act.

To carry out its responsibilities for the security of geographic areas around ports, the Coast Guard has designated a captain of the port within each of 43 geographically-defined port areas. The captain of the port is responsible for overseeing the development of the security plans within each of these port areas. In addition, maritime security committees, made up of key stakeholders, are to identify critical port infrastructure and risks to the port areas, develop mitigation strategies for these risks, and communicate appropriate security information to port stakeholders. As part of their duties, these committees are to assist the Coast Guard in developing port area maritime security plans. The Coast Guard is to develop a risk-based security assessment during the development of the port area maritime security plans

[3] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).
[4] Pub. L. No. 113–274 (Dec. 18, 2014).
[5] Pub. L. No. 107–295 (Nov. 25, 2002).

that considers, among other things, radio and telecommunications systems, including computer systems and networks that may, if damaged, pose a risk to people, infrastructure, or operations within the port.

In addition, under MTSA, owners and operators of individual port facilities are required to develop facility security plans to prepare certain maritime facilities, such as container terminals and chemical processing plants, for deterring a transportation security incident. The implementing regulations for these facility security plans require written security assessment reports to be included with the plans that, among other things, contain an analysis that considers measures to protect radio and telecommunications equipment, including computer systems and networks.

MTSA also codified the Port Security Grant Program, which is to help defray the costs of implementing security measures at domestic ports. Port areas use funding from this program to improve port-wide risk management, enhance maritime domain awareness, and improve port recovery and resilience efforts through developing security plans, purchasing security equipment, and providing security training to employees. FEMA is responsible for administering this program with input from Coast Guard subject-matter experts.

THE NATION AND ITS PORTS FACE AN EVOLVING ARRAY OF CYBER-BASED THREATS

Like threats affecting other critical infrastructures, threats to the maritime IT infrastructure are evolving and growing and can come from a wide array of sources. Risks to cyber-based assets can originate from unintentional or intentional threats. Unintentional threats can be caused by, among other things, natural disasters, defective computer or network equipment, software coding errors, and careless or poorly-trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled insiders, foreign nations engaged in espionage and information warfare, and terrorists.

These adversaries vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary gain or pursuing a political, economic, or military advantage. For example, adversaries possessing sophisticated levels of expertise and significant resources to pursue their objectives—sometimes referred to as "advanced persistent threats"—pose increasing risks. They make use of various techniques—or exploits—that may adversely affect Federal information, computers, software, networks, and operations, such as a denial of service, which prevents or impairs the authorized use of networks, systems, or applications.

Reported incidents highlight the impact that cyber attacks could have on the maritime environment, and researchers have identified security vulnerabilities in systems aboard cargo vessels, such as global positioning systems and systems for viewing digital nautical charts, as well as on servers running on systems at various ports.

In some cases, these vulnerabilities have reportedly allowed hackers to target ships and terminal systems. Such attacks can send ships off course or redirect shipping containers from their intended destinations. For example, according to Europol's European Cybercrime Center, a cyber incident was reported in 2013 (and corroborated by the FBI) in which malicious software was installed on a computer at a foreign port. The reported goal of the attack was to track the movement of shipping containers for smuggling purposes. A criminal group used hackers to break into the terminal operating system to gain access to security and location information that was leveraged to remove the containers from the port.

DHS AND OTHER STAKEHOLDERS HAVE TAKEN LIMITED ACTIONS TO ADDRESS MARITIME PORT CYBERSECURITY

In June 2014 we reported that DHS and the other stakeholders had taken limited steps with respect to maritime cybersecurity.[6] In particular, risk assessments for the maritime mode did not address cyber-related risks; maritime-related security plans contained limited consideration of cybersecurity; information-sharing mechanisms shared cybersecurity information to varying degrees; and the guidance for the Port Security Grant Program did not take certain steps to ensure that cyber risks were addressed.

Maritime Risk Assessment Did Not Address Cybersecurity

In its 2012 National Maritime Strategic Risk assessment, which was the most recent available at the time of our 2014 review, the Coast Guard did not address

[6] GAO–14–459.

cyber-related risks to the maritime mode. As called for by the NIPP, the Coast Guard completes this assessment on a biennial basis, and it is to provide a description of the types of threats the Coast Guard expects to encounter within its areas of responsibility, such as ensuring the security of port facilities, over the next 5 to 8 years. The assessment is to be informed by numerous inputs, such as historical incident and performance data, the views of subject-matter experts, and risk models, including the Maritime Security Risk Analysis Model, which is a tool that assesses risk in terms of threat, vulnerability, and consequences.

However, we found that while the 2012 assessment contained information regarding threats, vulnerabilities, and the mitigation of potential risks in the maritime environment, none of the information addressed cyber-related risks or provided a thorough assessment of cyber-related threats, vulnerabilities, and potential consequences. Coast Guard officials attributed this gap to limited efforts to develop inputs related to cyber threats to inform the risk assessment. For example, the Maritime Security Risk Analysis Model did not contain information related to cyber threats. The officials noted that they planned to address this deficiency in the next iteration of the assessment, which was to be completed by September 2014, but did not provide details on how cybersecurity would be specifically addressed.

We therefore recommended that DHS direct the Coast Guard to ensure that the next iteration of the maritime risk assessment include cyber-related threats, vulnerabilities, and potential consequences. DHS concurred with our recommendation, and the September 2014 version of the National Maritime Strategic Risk Assessment identifies cyber attacks as a threat vector for the maritime environment and assigns some impact values to these threats. However, the assessment does not identify vulnerabilities of cyber-related assets. Without fully addressing threats, vulnerabilities, and consequences of cyber incidents in its assessment, the Coast Guard and its sector partners will continue to be hindered in their ability to appropriately plan and allocate resources for protecting maritime-related critical infrastructure.

Maritime Security Plans' Consideration of Cybersecurity Was Limited

As we reported in June 2014, maritime security plans required by MTSA did not fully address cyber-related threats, vulnerabilities, and other considerations. Specifically, three area maritime security plans we reviewed from three high-risk port areas contained very limited, if any, information about cyber-threats and mitigation activities. For example, the three plans included information about the types of information and communications technology systems that would be used to communicate security information to prevent, manage, and respond to a transportation security incident; the types of information considered to be sensitive security information; and how to securely handle such information. They did not, however, identify or address any other potential cyber-related threats directed at or vulnerabilities in these systems or include cybersecurity measures that port-area stakeholders should take to prevent, manage, and respond to cyber-related threats and vulnerabilities.

Similarly, nine facility security plans from the non-Federal organizations we met with during our 2014 review generally had very limited cybersecurity information. For example, two of the plans had generic references to potential cyber threats, but did not have any specific information on assets that were potentially vulnerable or associated mitigation strategies. Officials representing the Coast Guard and non-Federal entities acknowledged that their facility security plans at the time generally did not contain cybersecurity information.

Coast Guard officials and other stakeholders stated that the area and facility-level security plans did not adequately address cybersecurity because the guidance for developing the plans did not require a cyber component. Officials further stated that guidance for the next iterations of the plans, which were to be developed in 2014, addressed cybersecurity. However, in the absence of a maritime risk environment that addressed cyber risk, we questioned whether the revised plans would appropriately address the cyber-related threats and vulnerabilities affecting the maritime environment.

Accordingly, we recommended that DHS direct the Coast Guard to use the results of the next maritime risk assessment to inform guidance for incorporating cybersecurity considerations for port area and facility security plans. While DHS concurred with this recommendation, as noted above, the revised maritime risk assessment does not address vulnerabilities of systems supporting maritime port operations, and thus is limited as a tool for informing maritime cybersecurity planning. Further, it is unclear to what extent the updated port area and facility plans include cyber risks because the Coast Guard has not yet provided us with updated plans.

Information-Sharing Mechanisms Varied in Sharing Cybersecurity Information

Consistent with the private-public partnership model outlined in the NIPP, the Coast Guard helped establish various collaborative bodies for sharing security-related information in the maritime environment. For example, the Maritime Modal Government Coordinating Council was established to enable interagency coordination on maritime security issues, and members included representatives from DHS, as well as the Departments of Commerce, Defense, Justice, and Transportation. Meetings of this council discussed implications for the maritime mode of the President's Executive order on improving critical infrastructure cybersecurity, among other topics.

In addition, the Maritime Modal Sector Coordinating Council, consisting of owners, operators, and associations from within the sector, was established in 2007 to enable coordination and information sharing. However, this council disbanded in March 2011 and was no longer active, when we conducted our 2014 review. Coast Guard officials stated that maritime stakeholders had viewed the sector coordinating council as duplicative of other bodies, such as area maritime security committees, and thus there was little interest in reconstituting the council.

In our June 2014 report, we noted that in the absence of a sector coordinating council, the maritime mode lacked a body to facilitate National-level information sharing and coordination of security-related information. By contrast, maritime security committees are focused on specific geographic areas.

We therefore recommended that DHS direct the Coast Guard to work with maritime stakeholders to determine if the sector-coordinating council should be reestablished. DHS concurred with this recommendation, but has yet to take action on this. The absence of a National-level sector coordinating council increases that risk that critical infrastructure owners and operators will be unable to effectively share information concerning cyber threats and strategies to mitigate risks arising from them.

Port Security Grant Program Did Not Take Key Steps to Effectively Address Cyber Risks

In 2013 and 2014 FEMA identified enhancing cybersecurity capabilities as a funding priority for its Port Security Grant Program and provided guidance to grant applicants regarding the types of cybersecurity-related proposals eligible for funding. However, in our June 2014 report we noted that the agency's National review panel had not consulted with cybersecurity-related subject-matter experts to inform its review of cyber-related grant proposals. This was partly because FEMA had downsized the expert panel that reviewed grants. In addition, because the Coast Guard's maritime risk assessment did not include cyber-related threats, grant applicants and reviewers were not able to use the results of such an assessment to inform grant proposals, project review, and risk-based funding decisions.

Accordingly, we recommended that DHS direct FEMA to: (1) Develop procedures for grant proposal reviewers, at both the National and field level, to consult with cybersecurity subject-matter experts from the Coast Guard when making funding decisions, and (2) use information on cyber-related threats, vulnerabilities, and consequences identified in the revised maritime risk assessment to inform funding guidance for grant applicants and reviewers.

Regarding the first recommendation, FEMA officials told us that since our 2014 review, they have consulted with the Coast Guard's Cyber Command on high-dollar value cyber projects and that Cyber Command officials sat on the review panel for 1 day to review several other cyber projects. FEMA officials also provided examples of recent field review guidance sent to the captains of the port, including instructions to contact Coast Guard officials if they have any questions about the review process. However, FEMA did not provide written procedures at either the National level or the port area level for ensuring that grant reviews are informed by the appropriate level of cybersecurity expertise. FEMA officials stated the fiscal year 2016 Port Security Grant Program guidance will include specific instructions for both the field review and National review as part of the cyber project review.

With respect to the second recommendation, since the Coast Guard's 2014 maritime risk assessment does not include information about cyber vulnerabilities, as discussed above, the risk assessment would be of limited value to FEMA in informing its guidance for grant applicants and reviewers. As a result, we continue to be concerned that port security grants may not be allocated to projects that will best contribute to the cybersecurity of the maritime environment.

In summary, protecting the Nation's ports from cyber-based threats is of increasing importance, not only because of the prevalence of such threats, but because of the ports' role as conduits of over a trillion dollars in cargo each year. Ports provide a tempting target for criminals seeking monetary gain, and successful attacks could potentially wreak havoc on the National economy. The increasing dependence of

port activities on computerized information and communications systems makes them vulnerable to many of the same threats facing other cyber-reliant critical infrastructures, and Federal agencies play a key role by working with port facility owners and operators to secure the maritime environment. While DHS, through the Coast Guard and FEMA, has taken steps to address cyber threats in this environment, they have been limited and more remains to be done to ensure that Federal and non-Federal stakeholders are working together effectively to mitigate cyber-based threats to the ports. Until DHS fully implements our recommendations, the Nation's maritime ports will remain susceptible to cyber risks.

Chairman Miller, Ranking Member Vela, and Members of the subcommittee, this concludes my prepared statement. I would be pleased to answer any questions you may have at this time.

Mrs. MILLER. Thank you very much.

The Chair now recognizes Mr. Parsons. Again, sir, we appreciate you traveling from California to join us today.

STATEMENT OF RANDY D. PARSONS, DIRECTOR, SECURITY SERVICES, PORT OF LONG BEACH, CALIFORNIA

Mr. PARSONS. Thank you, Madam Chair.

I appreciate the opportunity to provide some information this morning from an operations perspective. As you mentioned, the Port of Long Beach is the second-busiest seaport in the United States. Combined with our neighbor adjacent, the Port of Los Angeles, we handled over 15 million cargo containers in 2014. That represents over 40 percent of the imported cargo to the United States. Partly in effort to protect the diverse and large environment that we have, we operate the Joint Command and Control Center, which is a 24/7 operation. It provides domain awareness to all of our partners, Government and private sector, and is the hub for critical incident management. The coordination center houses over $100 million in technical security assets.

But we know the port authorities aren't the only target and possibly not the primary target for cybersecurity threats. Private-sector business entities, such as the terminal operators, control a substantial portion of the economic movement through our ports. The potential perpetrators and the threats, as you mentioned and as the admiral alluded to, aren't very unique to the maritime environment. We have threats to the port that are a danger to humans as well as catastrophic economic damage. We have workers. We have visitors. Both ports are housed in a densely-populated metropolitan area. Taking into account the dangerous nature of the persons—and the Port of Long Beach supports 30,000 jobs in the immediate area and 1.4 million jobs Nation-wide—an impact to a complex the size of Long Beach and Los Angeles could impact our National well-being. There are a number of challenges that we face in the maritime environment for cybersecurity.

There is not a one-size-fits-all solution for all ports. The business models for ports vary based on the size of the ports, the nature of the business that goes through the ports and, frankly, how they are governed. Long Beach is a landlord port. We have very little input into the security posture of our tenants. Other ports are operators of ports and are better postured to make recommendations and requirements.

A challenge is a lack of awareness about our own systems. Sometimes systems are a patchwork of legacy systems. They are often operated or administered by folks with different purposes and a

myopic focus on their required specific functions. This creates a lack of enterprise perspective or awareness for the cybersecurity problem. There is a notable reluctance to share information about cybersecurity issues. To acknowledge a cybersecurity event could potentially mean a loss of business reputation and public trust. Much of the information for maritime stakeholders is deemed as proprietary to the degree that dissemination could create business disadvantage.

There is a need to clearly identify roles and responsibilities of the various Government agencies involved in cybersecurity. The Ports of Long Beach and Los Angeles have been contacted and have worked with the United States Coast Guard, the FBI, Secret Service, and multiple entities of the Department of Homeland Security. We have tried to use incentives at our port to generate buy-in. We have done that successfully with our Green Port Program and our Clean Trucks Policy.

Now, FEMA has incentivized, to a degree, cybersecurity matters by emphasizing cybersecurity mitigation and vulnerability assessments in the recent grant year. We agree that subject-matter experts need to have continued input into those grant awards. The spending has increased as a result of that, but it is imperative that FEMA maintain a focus on strategic thought and the current and developing regulations. We support the efforts of the Coast Guard in their expanded mission to enhance security. But we realize that has created a specialized mission requirement that requires additional funding. We believe that protecting U.S. ports must be a core capability of our Nation. We realize, as everyone does, we cannot stop all attacks. But focusing on the development of strategic policies and guidelines is sorely needed. A roadmap that provides guidance but flexibility for industry decisions makes sense and will strengthen our National security cybersecurity posture. Thank you for the opportunity.

[The prepared statement of Mr. Parsons follows:]

PREPARED STATEMENT OF RANDY D. PARSONS

OCTOBER 8, 2015

Chairman and Members of the committee. My name is Randy Parsons and I am the director of security services for the Port of Long Beach, in California. Thank you for the opportunity to speak before the House Homeland Security Committee to discuss cybersecurity in the maritime environment from a field operations perspective, especially during October, National Cybersecurity Awareness Month.

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. 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 2014, the Port of Long Beach moved over 6.8 million 20-foot equivalent units (TEUs) of cargo, also known as containers. In August of this year, we experienced the highest volume of cargo in the Port's 104-year history.

Combined with our neighbor, the Port of Los Angeles, both ports comprise the San Pedro Bay Complex, the largest port complex in the Nation and the ninth-largest port complex in the world. Both ports moved over 15 million TEUs in 2014, which accounts for over 40 percent of the Nation's imported cargo. A 2010 report commissioned by the two 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 sheer volume of cargo moved throughout the port complex and transportation-related activities, protecting the San Pedro Bay Ports is vital to our National economic and security interests.

SECURITY

Safety and security are top priorities at the Port of Long Beach. Since September 11, 2001, the Port along with the other Government agencies responsible for security, have greatly expanded their efforts to protect the Port complex and surrounding communities. 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. My professional experience has been in recognizing threat situations and trying to formulate the best mitigation strategies. I have made observations, learned lessons from our own port operations and through contact with other local port partners, other ports, and transportation agencies.

The Port's Joint Command and Control Center, a 24-hour-a-day maritime domain awareness (monitoring) 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. The Port of Long Beach has formalized agreements 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. Law enforcement operations within the Port have been fully integrated between the Port of Long Beach Harbor Patrol and the Long Beach Police Department.

CYBERSECURITY

In 21st Century America, the Port of Long Beach, like many if not all organizations, relies heavily on information technology. The Port relies on information technology to operate the business of the port, as well as to secure the port complex and its assets. The maritime sector, like other industries are at risk for cyber attack, in part because ports are National economic drivers, and therefore are National critical infrastructures. That is why, in addition to the above water, on water, and underwater security monitoring and threat detection, cybersecurity has become a critical endeavor for the Port.

Port business operations and port authorities are not the only targets. Private-sector business entities, such as terminal operators, control a substantial portion of the economic movement through a wide variety of facilities. In the San Pedro Bay Ports complex, major cyber threat areas include port 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. Threats to the maritime environment include hacking, jamming, phishing, spoofing, malicious programs, taking control, and denial of service. On average, the Port of Long Beach's Information Management staff reports' thwarting 1 million hacking attempts a day. Some of the motivating factors for cyber criminal activities may involve smuggling, cyber extortion, gaining business advantage, intellectual property theft, and disrupting or destroying a National critical infrastructure. In addition to man-made cyber threats, the maritime sector is also susceptible to natural hazards such as earthquakes, hurricanes, and tsunamis.

Cyber threats do not necessarily target people to cause injuries and/or death, as with more traditional forms of terrorism. However, threats to ports 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, if not more, than other types of attacks. Large-scale, multi-pronged attacks in the cyber world will require a certain level of technical knowledge. However the logistics involved in cyber attacks may not rise to the level that was required for the September 11 attacks. Cyber attacks on such a large scale would create fear, instability, disrupt the normal way of life and business, and generate a lack of confidence in our Government's ability to protect us. These are some of the same goals of more "traditional" terrorist acts.

As a result, the maritime sector must adapt to a new threat environment as we have done constantly since the September 11 attacks.

It may seem overdramatic to make a comparison to the September 11 attacks, but one similarity may be in the number of cyber attacks that have taken place internationally and within the United States, as well as our responses, or lack of, to those warnings. As a result, business resiliency has become a critical part of our on-going cybersecurity plan. Reducing the potential for single-point failure, building redundancy into systems, and developing 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. Response teams must have specialized training and be prepared to engage 24/7. Protocols should include who receives notice of the event and what additional assets are available to assist. In a port environment, resiliency involves the ability of the logistics chain (public or private) to absorb the impact of business interruption caused by stress to the system (natural or man-made) and continue to provide 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.

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 ports are diverse in how their business is modeled. A lack of awareness about an organization's own systems creates opportunities for exploitation at a basic level. Systems themselves can be a patchwork of legacy systems, some integrated with newer technologies. Cyber systems can be administered by operators with different purposes and a myopic focus on only their required function (i.e. engineers, information technology, trade, human resources, and security). This creates a lack of an enterprise view of operations, which can lead to the "siloing" effect. The "siloing" effect is not an information technology problem, it is a "culture think" issue that takes effort to divest and generate a unified and collaborative perspective. At the Port of Long Beach, there is a continuing effort to align the enterprise Information Management function with the special needs of the Security Division.

In the maritime industry, there is a notable reluctance to share information about cybersecurity issues. To acknowledge that a cyber event has taken place could potentially diminish business reputation and public trust. Maritime stakeholders have deemed much of their information as proprietary to the degree that dissemination could create business disadvantages. Although this is a valid concern, it must be measured against the National security impact to a port complex like the San Pedro Bay. Not sharing cybersecurity information makes it difficult to identify the nature of threats or establish lessons learned and best practices to mitigate them.

There is not a clear or defined role and scope of responsibilities for the various Government agencies on the cybersecurity team. It is generally understood that, in substantial criminal cyber activity and terrorism matters, the Federal Bureau of Investigation (FBI) is the lead agency. However, the Ports of Long Beach and Los Angeles along with some of the tenants have been contacted by, and have also worked with the U.S. Coast Guard, the Secret Service, and multiple entities of Department of Homeland Security on cyber matters. Port authorities are willing partners in the fight against cyber attacks, however, there are requests for access to data from more than one agency. It is challenging to understand what type of cyber information is reported to which agency and duplicate requests for reporting often occur. This can be especially disconcerting for the private-sector entities whose proprietary concerns are heightened when multiple releases create more opportunity for compromise.

INCENTIVES

There seems to be clear recognition that serious cybersecurity concerns exist in the business world. However, left to our own devices, the business world seems not to be motivated to take the substantial action necessary to address those concerns in a strategic and collaborative manner. Thought should be given to the Federal Government creating incentives for businesses to enhance their cybersecurity efforts in a collaborative way. It is recommended that incentives be explored based on compliance standards. Uniformed guidelines, recommendations, and requirements are needed throughout the maritime sector. In order to gain "buy-in" from key stakeholders, the Port of Long Beach has found that industry incentives have been critical to the success of programs like our Green Port Policy and Clean Air Action

Plan. In general, businesses are reluctant to spend money on efforts that are not revenue-generating, even if there is a risk assessment indicating mitigation efforts could be revenue-saving.

The Federal Emergency Management Agency (FEMA) has incentivized cybersecurity activities by placing emphasis within the Port Security Grant Program (PSGP) on grant applications that focus on cybersecurity mitigation. It is important that cybersecurity subject-matter experts continue to be involved in the review process for these grant awards. It would be ideal to have that expertise engaged with FEMA practitioners who ensure decisions on cyber projects, as with all projects, continues to be driven by risk-based factors.

As a result of this grant prioritization, spending on cybersecurity has increased. FEMA should ensure that spending is in line with strategic thought and prevailing guidelines as they are developed. An example of focusing on priority projects has been the PSGP emphasis on cyber vulnerability assessments. The Port of Long Beach, Security Division is currently undergoing a comprehensive cybersecurity vulnerability assessment to enhance our posture. As we look to the future and contemplate industry regulations for cybersecurity measures, consideration must be given for continuing grant support to assist maritime security partners addressing the regulations, particularly if the regulations should be mandatory.

Collaboration between Government and the insurance industry could create incentives to protect valuable data identified by risk assessment modeling. When certain guidelines or industry standards are met, this could be reflected in premium costs. If incentives, and potential human and economic losses, are not motivation enough, a system of enforceable regulations or requirements may be necessary. Determining who would be covered by the rules and regulations is a fundamental question that will need to be answered. Specifically, the industry is interested in knowing whether the rules will apply only to facilities and vessels as with other regulations, or expand to other port enterprises.

The Port of Long Beach, concurs with the American Association of Port Authorities recommendation that there be flexibility in how policies are implemented to reflect the varying and evolving threat environment of similarly-situated ports. For example, U.S. ports can be either operators of a port or landlords with minimal input into operations. There are varying models of governance for ports that directly affect how port authorities interact with port partners like terminal operators, railroads, trucking companies, and shipping lines.

NATIONAL CYBERSECURITY POLICY

The Port of Long Beach supports efforts for the U.S. Coast Guard to realize their new mission to lead the effort in enhancing cybersecurity in the maritime environment. The U.S. Coast Guard and the Captains of the Port are in the best position to facilitate and coordinate the drafting of regulations, cybersecurity awareness programs, vulnerability assessments, training, clarification of roles and responsibilities, exercises, and information sharing. In this role, the U.S. Coast Guard can provide a strategic view for cybersecurity in a maritime environment, identify lessons learned and best practices, and coordinate efforts among port industry stakeholders.

The U.S. Coast Guard focus on cybersecurity in the maritime sector has created a need for specialized mission requirements. Those requirements must be supported through adequate funding for the U.S. Coast Guard to develop and acquire subject-matter experts and equipment 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 Cybersecurity. Coordination between NIST and the Coast Guard 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.

SOLUTIONS

Solutions to these cybersecurity challenges exist. All entities must take inventory and identify their own systems and capabilities. This includes identifying employee and contractor access and duties to port facilities and information systems. In assessing impacts, it has been identified that people cause the most damage. Once cyber operations are understood on an enterprise scale, systems and protocols can be organized to promote cybersecurity throughout the organization. Legacy systems can be evaluated for updating to meet today's, and more importantly, tomorrow's 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 effecting key operations. The Port of Long Beach, Security Division is undergoing a comprehensive assessment; it will be the third such assessment in 3 years.

Cybersecurity training and educational programs must be robust and continual. Training should include prevention, detection, response, and recovery efforts and procedures. Presentations are more meaningful if they contain real-world incidents and reporting. Case studies and examples are particularly valuable when they focus on lessons learned and best practices. System operators need to know what a potential cyber incident looks like and how it behaves. This type of training provides awareness for port industry leaders and employees to create a "See Something/Say Something," environment in the cyber arena. The benefits received from a collaborative environment promote information sharing.

Another layer to cyber preparedness is conducting tests, drills, and exercises, as with other critical or emergency situations. In 2014, the Port of Los Angeles hosted a large, multi-agency, full-field cybersecurity exercise. Lessons were learned from integrating cyber threats with real-world operations. Drills and exercises for cybersecurity teams should be commonplace and testing of all employees should happen throughout the year, not just during Cybersecurity Month in October.

When cyber events occur, decisions must be driven by information. Collaboration that produces an environment of sharing information will include balancing the need to protect propriety information with protecting our National critical infrastructures. The city of Los Angeles created a Cybersecurity 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 U.S. Coast Guard, Sector Los Angeles/Long Beach, Area Maritime Security Committee has approved a Cyber Security Subcommittee and we look forward to its launch and being an active participant.

Information sharing can be facilitated by clarifying roles and responsibilities for all cybersecurity players including local, State, Federal governments and private sector. This clarification must be shared with the entire maritime community. When an event is detected, proper notifications must be made, mitigation efforts are initiated, and an investigation may begin. Agency responsibilities may differ for each of these tasks and that must be understood by all. Likewise, lines of communication should be clear about who will analyze the information and identify potential perpetrators, techniques, and patterns or trends. If these efforts generate information of value, it must also be determined which agency disseminates the information and how it is disseminated.

The reporting of cybersecurity-related information has not been a two-way flow of information sharing, it has mainly been the maritime sector providing information to Federal Government agencies. There should be a concerted effort to evaluate and identify information that can be released to the proper audience to keep them "in-the-loop." This feedback is critical for identifying lessons learned, best practices, and foster the critical sharing relationship. One bright spot has been the collaboration between the ports of Long Beach and Los Angeles and the FBI's Cyberhood Watch Program. This is a program where cyber information is shared by port partners, including private-sector partners, with the FBI. The FBI analyzes the data for suspicious behaviors and the results are shared back with the contributors and all partners in the program. The FBI will also take further investigative steps when warranted.

CONCLUSION

It is important to recognize that while we vigorously try, we cannot stop all attacks. 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 strategic policies and guidelines 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 for the opportunity to address you on behalf of the Port of Long Beach. I would be pleased to take any questions.

Mrs. MILLER. Thank you very much.

The Chair now recognizes Mr. Sawicki. Again, we appreciate you traveling from Texas to join us, sir.

STATEMENT OF JONATHAN SAWICKI, SECURITY IMPROVEMENT PROGRAM MANAGER, PORTS OF BROWNSVILLE AND HARLINGEN, TEXAS

Mr. SAWICKI. Thank you very much.

Madam Chairman, distinguished Members of the committee, and Members of the audience, my name is John Sawicki. I was asked to testify today based upon experience gained while serving as a security improvement program manager for the Ports of Brownsville and Harlingen, Texas. I am humbled and honored to be here today to share with you this experience, as well as my own opinions on the status of cybersecurity in our port communities. Today, I would like to focus on the importance of risk-based, strategic planning and how cyber risk is a critical component within that approach. I would like to share with the committee information on recent efforts to manage cyber risk in the maritime domain and will provide brief comments on the Coast Guard's cybersecurity strategy, as well as provide some general recommendations for consideration.

My hope today is that once we all leave here, the Members of the subcommittee, the audience, and my fellow witnesses are better equipped to make informed risk-based decisions when implementing cybersecurity and resiliency strategies. The bombing of the U.S.S. Cole and September 11 attacks on our country made it clear that we had to increase our level of homeland security Nation-wide. Just as how we travel by air has changed, the way we conduct maritime commerce has also changed.

We need to understand, we all know that there are capable and motivated threats out there for cyber and for physical security. We must implement risk-based strategies. To mitigate against some of these physical security threats, in 2002, the Port of Brownsville established a sworn police department responsible for not only enforcing laws and providing public safety but for implementing programs and measures to protect port infrastructure and maintain compliance with the MTSA. In 2007, the port conducted a comprehensive threat assessment, which was closely followed by a port-wide strategic risk-management plan in 2008.

While not required of the Port of Brownsville, this plan has been a critical component to our success with the Port Security Grant Program, securing over $14 million in funds for physical security enhancement projects. Currently, the port is in the process of updating this initial port-wide strategic risk management plan with an additional focus on industrial hazards and cybersecurity. A strategic risk-based approach to managing the threats and hazards at the Port of Brownsville has resulted in a safer and more secure environment within which commerce can be conducted.

Cybersecurity, Port of Brownsville. Using the NIST Cybersecurity Framework as a guide, the Port of Brownsville recently conducted a cybersecurity assessment to identify critical systems, evaluate current cybersecurity posture, establish a target state for cybersecurity, and identify and prioritize opportunities for improvements. The timing of this assessment was optimal, as the port had recently hired its first IT manager and was in the process of per-

forming significant upgrades to existing communication systems, port management systems, and general operating systems.

The result of this cybersecurity assessment indicated opportunities for improvement in all five cybersecurity functions: Identify, protect, detect, respond, and recover. Using the results of this assessment, the port prepared and submitted a grant application through the fiscal year 2015 Port Security Grant Program. Unfortunately, the project was not funded. Even though it was not funded, the port strives to improve our cybersecurity posture and, even though at a slower pace, is doing so.

Comments on the U.S. Coast Guard strategy. In general, I support the U.S. Coast Guard's vision for operating in the cyber domain and the three primary priorities of defending cyber space, enabling operations, and protecting infrastructure critical to the MTS. The risk-based decision-making model utilized in the overall strategy development and proposed implementation will be very beneficial. I believe that the stated goals and objectives are reasonably achievable, given support and resources on an on-going and consistent manner. I think that on-going and consistency is very important. The most important goal stated in the strategy in terms of port-wide risk management in my mind is to increase operational resiliency by ensuring mission-focused cyber space operations and incorporating cybersecurity into U.S. Coast Guard culture. This focus on resiliency and the concept of establishing a culture of cybersecurity is key to managing risks posed by a persistent and capable threat. This operational resiliency will effectively reduce the consequences associated with a potential cyber-based transportation security incident and work to gain buy-in from port area partners and other maritime domain stakeholders. Ultimately, to adequately address the cyber risk, we must all work to establish and nourish a culture of enhanced cybersecurity and vigilance within our own organizations. You have many of my recommendations in my written testimony, so I am not going to go through all those today. But, most importantly, I feel we need to continue to support at the port level and the National-level risk-based decision making and the assessments required to do so.

So I will leave you today with thanking you for this opportunity. General Douglas MacArthur is credited with saying: There is no security on this Earth, only opportunity. I feel right now we have that opportunity to help build cybersecurity throughout the MTS. Thank you very much.

[The prepared statement of Mr. Sawicki follows:]

PREPARED STATEMENT OF JONATHAN SAWICKI

OCTOBER 8, 2015

INTRODUCTION

Madam Chairman, distinguished Members of the committee and members of the audience, my name is Jon Sawicki and I was asked to testify today based upon experience gained while serving as the security improvement program manager for the Ports of Brownsville and Harlingen, both located in Cameron County, Texas. I am humbled and honored to be here today to share with you this experience, as well as my own opinions on the status of cybersecurity in our port communities.

Today I would like to focus on the importance of risk-based strategic planning and how cyber risk is a critical component of that approach. I would like to share with the committee information on recent efforts to manage cyber risk in the maritime

domain and will provide brief comments on the USCG's Cyber Strategy, as well as provide some general recommendations for consideration by the USCG and committee Members as you work to enhance the National cybersecurity posture. My hope today is that, the Members of the subcommittee, the audience and my fellow witnesses are better equipped to make informed risk-based decisions when developing and implementing cybersecurity and resiliency strategies.

STRATEGIC PLANNING AT THE PORT OF BROWNSVILLE

The bombing of the USS Cole on October 12, 2000, and the subsequent terrorist attacks against the United States on September 11, 2001 made it clear that homeland security as a whole needed to be enhanced throughout our country. Just as how we travel by air has changed significantly, the means by which we conduct maritime commerce in ports and waterways world-wide has been impacted by the reality that motivated and capable threats do exist, and they pose a risk to the lives and livelihoods of people everywhere.

To mitigate against physical security threats, in 2002 the Port of Brownsville established a sworn police department responsible for not only enforcing laws and providing public safety, but for implementing programs and measures to protect port infrastructure and maintain compliance with the Maritime Transportation Security Act (MTSA). In 2007 the Port conducted a comprehensive threat assessment, closely followed in 2008 by the development of a port-wide strategic risk management/mitigation and trade resiliency/resumption plan, which has since been used as a guide for the design and development of PSGP project applications.

While not required of the Port of Brownsville, the completion of this first port-wide strategic risk management plan has been critical to our success in securing approximately $14,000,000 in funds to implement projects of a wide variety; from the development of sophisticated wide-area surveillance and TWIC-compliant access control systems; the construction of a new port command center and commercial truck entrance; and the purchase of multiple portable generators, light towers, and security shelters for use during incident response and disaster recovery operations.

The Port is currently in the process of updating the initial Port-wide strategic risk management/mitigation and trade resiliency/resumption plan. This update has an added focus on industrial hazards at non-USCG-regulated facilities, the ability to coordinate emergency response activities with all port tenants and evaluating the Port's cybersecurity and network preparedness posture. A strategic risk-based approach to managing the threats and hazards at the Port of Brownsville has resulted in a safer and more secure environment within which commerce can be conducted.

CYBERSECURITY AT THE PORT OF BROWNSVILLE

Using the National Institute of Standards and Technology (NIST) Cybersecurity Framework as a guide, the Port of Brownsville recently conducted a basic cybersecurity assessment to identify critical systems, evaluate their current cybersecurity posture; establish a target state for cybersecurity; and identify and prioritize opportunities for improvement within the context of a continuous and repeatable process. The timing of this assessment was optimal as the Port had recently hired its first in-house IT manager and was in the process of performing a significant upgrade to the existing communications platform, computer operating systems (hardware and software) and port management information system.

The results of the cybersecurity assessment indicated opportunities for improvement in all five cybersecurity functions; identify, protect, detect, respond, and recover. Using the results of the cybersecurity assessment the Port prepared and submitted a grant project application through the fiscal year 2015 PSGP, which unfortunately was not selected for funding. Though this project did not receive funding, the Port strives to improve cybersecurity and network resiliency through targeted upgrades and enhancing the capabilities of IT-tasked personnel.

USCG CYBERSECURITY STRATEGY

In general I support the USCG's vision for operating in the cyber domain, and the three primary priorities of defending cyber space, enabling operations and protecting Infrastructure critical to the maritime transportation system. The risk-based decision-making model utilized in the overall strategy development and proposed implementation will be beneficial, and I believe that the stated goals and objectives are reasonably achievable given support and resources are on-going and consistent.

The most important goal stated in the strategy in terms of port-wide risk management is to "increase operational resiliency" by ensuring mission-focused cyber space operations, and incorporating cybersecurity into U.S. Coast Guard culture. This focus on resiliency and the concept of establishing a culture of cybersecurity is key

to managing risk posed by a persistent and capable threat, or natural hazard such as a major hurricane. Given the likelihood of a future cyber incident impacting the maritime transportation system, the true measure of a successful cyber risk management program will be the ability to operate in a degraded manner while the threat is addressed and systems are restored. This operational resiliency will effectively reduce the consequence associated with a potential cyber-based transportation security incident, and work to gain buy-in from port-area partners and other maritime domain stakeholders. Ultimately, to adequately address the cyber risk we must all work to establish and nourish a culture of enhanced cybersecurity vigilance within our own organizations.

RECOMMENDATIONS AND CLOSING STATEMENT

Recommendations:

- Continue to provide resources through the PSGP to promote the enhancement of cybersecurity and network preparedness within the maritime domain. Considerations should be made to reduce the cost match requirement for cybersecurity assessments and strategic planning projects that follow the NIST Cybersecurity Framework.
- Continue to provide resources through the PSGP to conduct or update port-wide strategic risk management/mitigation and trade resiliency/resumption plans. Consider reducing the cost match requirement for grantee projects that directly address cyber vulnerabilities identified in the strategic risk management plans and/or area maritime security assessment (AMSA).
- Continue to provide resources through the PSGP to support cybersecurity training and exercises. Consider reducing the cost match requirements for projects that provide consistent and accredited cybersecurity training of varying levels to members of the port community, specifically those offered to both public and private entities.
- Provide for flexibility in future policies or regulations, taking into account unique port-specific risk profiles and operating environments when determining appropriate mitigation levels.
- Further define and provide guidance on what constitutes a transportation security incident specific to potential or actual cyber breaches.
- Encourage cybersecurity breach reporting by port facilities by putting in place measures to safeguard information to a degree that limits the reputational impact on the entity breached.
- Continue to lead and facilitate cybersecurity discussions at AMSC meetings and other industry groups such as ASIS and the FBI's Infraguard Program.

Thank you again for the opportunity to testify before this subcommittee. General Douglas MacArthur is credited with saying, "There is no security on this earth; only opportunity". These words are as relevant today as they were almost a century ago. Cybersecurity must be approached as an on-going cycle, not a means to an end. Threat actors will always look for opportunities to exploit system vulnerabilities. As such, we must always be identifying and capitalizing on opportunities to increase our own preparedness, protection, and response capabilities.

Mrs. MILLER. Thank you, all of you, gentlemen. I think what I will do is just ask a more global question and ask each one of you to respond to it. I will preface it by telling you the reason I called this hearing, obviously, I mean, if you talk to anybody at the Pentagon and you ask them, "What keeps you awake at night," they will tell you cyber attack. That is what they are worried about, as much as anything else, of all the threats that we face. When you talk to Members on the Intel Committee, you know, they will tell you about some of the things that are happening. I mean, we see some of the things openly reported of these hackers, like the OPM kind of thing that happened here in the Government domain recently, where you had the hackers sitting there probably in the information environment for could have been a year, you know. As Members of Congress, we were talking about whether or not we ought to get credit-security agencies available to all these folks that had been hacked in. But, look, they weren't looking for somebody's credit card information probably.

The other hat that I wear besides sitting on the Homeland Security Committee, I am also the Chair of the House Administration Committee, where we are concerned about cyber for the campus here. I won't go into some of the issues that we have had there. But, obviously, we are a target, right? So you can imagine.

But, at any rate, as I sort-of think about this whole area of cybersecurity in the port, in the maritime environment, and I think about the Coast Guard being missioned with this, and, Admiral Thomas, I would also say, you know, I also have a saying, I always say if it is wet and impossible, send in the Coast Guard because you guys just handle it. Then, you know, since 9/11, all we have done is load you up, load you up, load you up with so many other kinds of missions. Now you are tasked with this as well, with cybersecurity. But, you know, the world is a changing, evolving threat environment all the time. It is much more asymmetrical than it has ever been in the past, as evidenced by the kinds of things, the worries that fellows at the ports are having.

I guess, just generically, my question is: How do you think the Coast Guard is doing with this mission? To the rest of you—and nothing against the Coast Guard—but do you think the Coast Guard is the proper agency, and do they have adequate resources, again, to carry out another mission that the Government has missioned them, tasked them with? Our committee, we need to hear from all of you of what kinds of situations you are having out there. Then it is up to us to finance to the best extent that we can, prioritize the Government's money here of doing the kinds of things we need to be able to do to make sure that the missions we give the brave men and women in the Coast Guard and every other agency is adequate for that. I guess that is, sort of generally, I am trying to understand whether or not the Coast Guard is, the kinds of challenges that you find yourself with and what the rest of you think about how that is going and what, perhaps, we could do differently if necessary. Admiral?

Admiral THOMAS. Thank you for that great question. In my statement, I mentioned that we don't view this as a new mission. We view it as a natural extension of our existing mission. Maybe I can elaborate on that. When the maritime industry shifted from sail to steam, the Coast Guard had to develop standards and the ability to assure compliance with those standards for boilers and for engineers for the first time, and then when we shifted from steam to internal combustion and from internal combustion to major electrical power. So the industry has moved to operating in cyber. The Coast Guard has got to move with them. So it is the natural extension of our mission given to us by Congress to manage operational risks in the maritime area.

Now, that said, it is a different type of risk that we have to manage. So we need to develop different expertise, and we need to bring some different capabilities. We are doing that by leveraging the expertise and capabilities that exist across the Government and by building our own work force. One of the reasons why our commandant insisted that we have a cyber strategy is so that our entire organization stays focused on those things that we know we need to do in order to be operationally effective across all of our missions in the 21st Century operating environment. That includes

building the workforce. It includes developing the proper kind of standards. So, again, I don't see this as a new mission. We see it as a new domain in which we need to conduct all of our missions.

Certainly when I talk to the industry about how do we manage the risks introduced by cyber systems, and we talk about how we manage other risks that, you know, have always been out there, the same types of approaches, the same risk-based performance standards, the same type of regulatory regime is what people tell me they think works. So thank you for the question.

Mrs. MILLER. Mr. Wilshusen.

Mr. WILSHUSEN. Yes, I would just like to add, too, that it is good to hear Admiral Thomas talk about leveraging other resources across the Federal Government because there are several that can help as the Coast Guard tries to bring up their cybersecurity capabilities. Even within its own Department, the Department of Homeland Security, the Office of Cybersecurity and Communications has a number of groups that are skilled in cybersecurity-related matters, and that certainly can help inform the Coast Guard's effort. In addition, the National Institute of Standards and Technology has developed a framework, a cybersecurity framework for improving cybersecurity within the critical infrastructure. That, too, is another framework that can help inform the Coast Guard's efforts and, indeed, all of the maritime sectors' efforts to improve the cybersecurity. So there are other resources available that can help the Coast Guard in performing those activities.

Mrs. MILLER. Mr. Parsons, what is your thought?

Mr. PARSONS. Madam Chair, I don't think there is any question the Coast Guard is the right agency. The Coast Guard and their Captains of the Port are perfectly positioned to lead strategy and guidelines for port security measures. As the admiral says, that is what they have done all along. They are the right people.

Clearly, something this large and complex, there is going to be a maturational process to this. I feel like we are at the beginning of it. But the things that I feel we need in the maritime environment are leadership, coordination, a strategy, create a fabric for all the working entities in the port, not just port authorities but for the business entities in the port. Quite frankly, we struggle as a landlord port to have much say in the position of security in our tenants.

You mentioned the fully-automated terminal. Once fully operative, that will handle 3 million cargo containers a year. That number, which is expected to be fulfilled through contracts, would make that one terminal the fourth-largest port in the United States. We have very little input into their—we can inquire, we can discuss it, we can confer and collaborate. But we have no guidelines or standards that could help them motivate. I am sure they have a very robust cybersecurity program for a fully-automated terminal. But we don't have any insight into that and no real insight in how to get there. The last thing I would say is many of the challenges I mentioned, again, the Coast Guard I think is postured for systems awareness, threat awareness, training programs. They are kind-of a mishmash if they exist.

Our concern is that the level of resources that they have to do this job and how long it would take to do it. If there were a Na-

tional vulnerability assessment, a charge for all ports, that is going to be a beefy undertaking. It is going to take a long time. But, again, with their experience of understanding the difference between the different nature of the ports, I think the Captains of the Port are, again, the best postured to take something like that on.

Mrs. MILLER. Mr. Sawicki.

Mr. SAWICKI. Thank you very much. In my opinion, for the current operations, yes, the Coast Guard has resources to continue to facilitate the conversation. I think that is the most important part right now is that within ports, we have many experts at many private terminals. But it is very difficult to get them all into one room to share their own strategies because they all compete. So I think at this point, the Coast Guard is doing an incredible role through Area Maritime Security Committees, to port safety committees to facilitate that conversation and to better understand what private industry is doing, some of their concerns. The primary concern that I see with information sharing specifically with port tenants is the possibility for reputational impact of a private company if they share a cyber breach.

So I think, currently, by facilitating these conversations, by working with private industry and working within existing regulations, I believe the Coast Guard is the right organization for this role. I believe it will take us a while to get there, but this is a very big problem. We are still in the proactive stage. Fortunately, we are not in the reactive stage. Thank you very much.

Mrs. MILLER. Thank you all very much.

Before I recognize the Ranking Member, I would also like to recognize, and as you see, the gentleman from Texas, Mr. Ratcliffe, who is the Chairman of the committee's Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technology, be allowed to sit on the dais and participate in today's hearing.

Without objection, so ordered.

Mr. Vela.

Mr. VELA. Thank you, Madam Chairman.

Mr. Parsons, you hit on two points that I would like to basically hear about in a broader context of not just cybersecurity but port security in general. The first is with respect to communication between ports, for example, in California, Port of San Diego, Long Beach, Los Angeles, San Francisco, and many others—in Texas, it would be Port of Brownsville, Port of Corpus Christi, Galveston, Houston—what kind of information-sharing systems do we have in place between all these different ports?

Mr. PARSONS. In our area, we have, the first thing and the best thing is we know each other. We spend a lot of time together in other emergency management and crisis situations. We attend the same conferences. We are part of the same cybersecurity working groups that cover both ports. We share information.

I will tell you a bright spot in information sharing is the FBI's Cyberhood Watch Program. That is one place where port entities and, importantly, private-entity terminals have agreed to input their defense information as they defend against cyber attacks into the FBI Cyberhood Watch. The FBI analyzes that information. One thing we really appreciate is, it is a two-way flow of information. They provide the information back to the stakeholders if they see

a pattern or a trend that needs tending. That goes to all stakeholders. So some of that proprietary influence has been broken down with Cyberhood Watch.

Mr. VELA. Mr. Sawicki.

Mr. SAWICKI. I agree. It would also reinforce that through the FBI's InfraGard Program as well. That is where a lot of industry information sharing takes place. Port-wise, you are looking at conferences, AAPA events, seminars where the same groups get together, discuss issues they are sharing. I am not aware of any formal communication platform between ports to share. Now, if there is an issue, someone receives a breach, then information sharing takes place through the National Response Center. I have not seen that process take place. I am not sure how reactive it can be. But, currently, Area Maritime Security Committees, existing meetings, the conversations are happening. Everyone is talking about it. But as far as a formal platform, I am not aware of one.

Mr. VELA. So would the common thread from coast to coast be the FBI Cyber Watch Program? Is that what you called it?

Mr. SAWICKI. There are multiple programs under, I believe under the InfraGard Program which is, I am a member, I sign up, very quick background checks. Then I receive emails on specific threats that are out there. Most of these are Non-classified but Sensitive I guess would be the way to put it. So there is information in industry. When industry partners talked to non-maritime, like NERC, for example, some of the other regulatory boards, there is a lot of information out there. But it is more informal than formally received.

Mr. VELA. Mr. Parsons, the other point I wanted to hit on is you mentioned the challenge in getting the tenants to share information. Is that something that we see across the Nation?

Mr. PARSONS. Yes. One of those things I don't think is unique to the maritime environment. It is a valid concern. One thing I think the Cyberhood Watch Program has done is called the private-sector tenants together, made the point: We understand your position; we have seen it happen in the United States. But, on balance, with the port complex such as Long Beach and Los Angeles, we do have to balance proprietary interests with potential damage to National security. That argument and possibly others have drawn these private-sector people into Cyberhood Watch. That is a huge step. There has been a lack of trust, parochial interest in their information. That has been a tough pull. But this is a glimmer of success that we have seen.

Mr. VELA. Mr. Wilshusen, what are your thoughts on the 2015 Coast Guard cyber strategy?

Mr. WILSHUSEN. I think it is a step forward to recognize and identify the three objectives that they have laid out in their strategy, particularly with protecting the critical infrastructure in the maritime environment, which was the focus of our report and the actions we have done there. So, to that extent, I think it has been a positive step and something that, of course, I understand will be guiding their efforts going forward.

But one thing I would just like to also point out regarding the information-sharing issue that has been discussed is that there have been a number of barriers to effective information security.

Mr. Parsons and Mr. Sawicki touched on a couple of those. One is having, establishing those relationships and how important it is to establish trust in order for private-sector companies to share their information with the Government or among themselves. The other thing is part of what could happen to facilitate that sharing of information is to have a secure mechanism in which organizations can provide that information to Government and, conversely, Federal agencies can provide actionable threat alert and incident information back to the private sector. There should also be capabilities to anonymize the information so the issue with regard to reputational impairment, if you will, on the part of a private sector who reports an incident and it is cited, leads could be anonymized so the individual entity is not being identified, but the information about the threat, about the incident, and it will be something that can be shared across the sector. So there are a couple actions that can be taken to help improve information sharing across the board.

Mr. VELA. Thank you.

Mrs. MILLER. The Chair recognizes the gentleman from New York, Mr. Donovan.

Mr. DONOVAN. Thank you, Madam Chair.

I would like to thank you and the Ranking Member for allowing me and Ratcliffe to intrude on your hearing.

First of all, gentlemen, thank you for what you do for our country, your interest in protecting our National security. I have two reasons why I asked the Chairwoman and Ranking Member if I could join you today. One is we have a great love for the Coasties. I come from New York. When Governors Island closed, the Coasties came to Staten Island, where I live. We are very proud. We are very grateful for their work. We are so honored that they decided to come to Staten Island.

The other is my dad was a longshoreman for 40 years. Before containerization, longshoremen would go down into the hull of the ship with a hook and grab a burlap sack of coffee beans and walk it out of the hull of the ship. My father used to come home with the coffee beans, the loose ones, in his cuffs of his pants. We used to grind them up, and we had coffee. But, you know, the security back then, I suspect they had dogs that would sniff the cargo, maybe some detectors for radiological materials on some of the ships. But your mission has become so great.

When you spoke, Admiral, about—you guys remind me of Larry the Cable Guy; you are just going to get 'er done no matter what it is. But your resources are finite. To take on this other mission or expanding the mission that you already have in the security of our ports is going to cost you resources. Are other parts of the Coast Guard's missions going to suffer because now you have to direct resources to this new threat that we face now in cybersecurity?

Admiral THOMAS. Thanks for your support of the Coast Guard. We love Staten Island as well. I would say of the three objectives in our Coast Guard cyber strategy, the least resource-intensive is the one around our role for protecting maritime critical infrastructure. That is because of some points that have already been made. That infrastructure is privately-owned. The real responsibility to do the defense of those systems is with the private sector. So we don't envision Coast Guard personnel, for example, actively defending

private-sector systems. Our role in that regard is to set a reasonable performance standard and then have the people in place to ensure that standard is met. That might involve the use of third parties. In fact, I am quite certain that it would. We use third parties across our compliance program. So do we need additional resources to do that? Yes. Is the demand as large as you might think? Probably not, at least not for that component of our strategy because, again, we will leverage the capabilities across the Government, both in terms of setting the standards. One of the reasons that we don't have the assessments in place that the GAO would like to see is because we want to make sure we use the same assessment tools that are used in other sectors. They are just not there yet. So it wouldn't make any sense to move out ahead of them.

But we will leverage all those resources. Yes, there will be a resource bill. Will it impact our other missions? Our Coast Guard Commandant has been pretty clear that cyber is a way to make sure we do our missions better and more effectively. It is not a mission to detract from others.

Mr. DONOVAN. Thank you very much.

Madam Chairman, I waive the rest of my time. Thank you.

Mrs. MILLER. I thank the gentleman.

The gentlelady from California, Ms. Sanchez.

Ms. SANCHEZ. Thank you, Madam Chair. Once again, always a pleasure to serve with you on this subcommittee. As you know, I probably live about 25 minutes away from the Port of Long Beach and maybe half an hour away from the Port of Los Angeles. Almost 50 percent of our goods, I think, come through those two ports to the United States. The Port of Long Beach alone handles about $150 billion in trade annually. Of course, we are talking about a lot of Southern California jobs between these two ports.

So I would like to ask Mr. Parsons, what would be the impact of a significant cyber attack on your port? What do you envision would be, on the high end, something that would just cripple what is going on? How long do you think, given the current infrastructure, it would take to get things back to normal?

Mr. PARSONS. Congresswoman, we are always very concerned about major attacks. But I will tell you, we have experienced plenty of small ones that have given us some insight into what happens in port environments. Those have been generated some by labor action and slow downs, some by malfunctioning of systems, not only within ports but on a larger scale, with the city of Long Beach.

Ms. SANCHEZ. With the automation, and I know the automation—I understand the whole issue of much of this infrastructure is owned by these individual maritime companies, et cetera. But give me an example of something that you think would be just incredibly crippling and what we could imagine would be the aftereffect. I am thinking from an economy standpoint in particular for California.

Mr. PARSONS. Well, we could go back to 2002 and the work stoppage there, where the National economy was dramatically affected. Depending on whose figures you believe——

Ms. SANCHEZ. Was that like 8 days or 18 days?

Mr. PARSONS. Exactly. In 2002 dollars, it was a loss of $1 billion a day to the National economy. So we can assume it has gone up

from there. What we have seen is systems shut down. As Mr. Sawicki talked about, resiliency and redundancy is a huge part of cybersecurity; how quickly can we spin back up? What we have seen is a lack of redundancy and acceptable back-up systems, in some cases, as simple as power back-up. Some of the terminals, during the problems we had with the electrical grid out there, they were down. The irony was the security systems were up and running, were back up, but the economy isn't moving. So that is a great concern to us. Again, it goes back to the awareness of the systems; exactly how long would it take these individual terminals to come back on?

Ms. SANCHEZ. I remember it was, even after we solved the issue, it was a long time in getting the back-up and getting everything back to normal and getting the ships out. Of course, much of that was perishable to some extent, et cetera. So it was a big economic crunch.

I am very confident in my Coast Guard, I have visited a lot both up in the San Francisco Bay area and, of course, in our ports, and in San Diego, with respect to your ability to cover and to have consistent knowledge of each port within the Coast Guard. So I want to congratulate you on that actually because I think you are doing a good job with respect to that.

But I think this whole issue, Madam Chair, going back to this issue of, and we have seen this over and over in other areas, whether it is petrochemical or anything else, that the mainstay of the infrastructure is in individuals' hands, right, in private hands. So what is our role, and how do we ensure that, in fact, even in an economic situation there is backup energy generation, for example? So I know that you have all talked about, you know, we need more communication or we need more, we need to know more. How do we do that? How do we, if we, the Government, wanted to somehow take the initiative to actually get this going, what would that look like? What could we do, given that everybody, the individual stakeholders have proprietary information, you know, they want to but they don't want to come together and figure out how we are better protected against cyber. Seeming that Homeland Security is supposed to be in charge of everything but defense cyber in our agencies and that we are somehow supposed to help private entities who are so important to us get this act together with us, what would you suggest? If I told you tomorrow, "Fix this problem and let's get this done," what would that look like? To any of you who are on the panel. Give us some ideas of what we can do as a committee to help you get that done.

Mr. SAWICKI. It is a very good question, a very difficult question. But I think, initially, it is to focus on those systems that facilitate commerce, the navigation systems. You know, after a hurricane, as an example, you can have every facility ready to operate, but if that channel isn't open, then it really doesn't matter.

So I would say focus on the major navigation systems, the Federal systems. Ensure private industry's trust in those systems, and then help facilitate conversations among private industry because I believe private industry is going to do on their own to protect their own interest. So other than that magic bullet, it is just to

focus internally first while everyone else tries to get a handle on the situation on their own, if that makes sense.

Mr. PARSONS. Congresswoman, as a Government and a committee, it has a lot to do with what we talked about today: Supporting the Coast Guard to create this fabric; identify systems through risk-based assessments; identify the priority gaps. But I think there has got to be some regulation. It can be voluntary, as it has been in the past. To be honest with you, left to our own devices, we don't seem to have done very well.

So the other thing I mentioned is the Port of Long Beach has used incentives for our private-entity partners to engage in various programs that we have had there. But you may evolve to regulations and even requirements, authorities that have been given to the Coast Guard in some other areas, but we have to generate whatever motivation it's going to take to get this done.

The reason it is going to be a maturational process is there's not one size that fits all with ports, so there has got to be a recognition that it is a different playing field in different ports.

Ms. SANCHEZ. Thank you, Madam Chair.

Yes, and I agree. If you have seen one port, you have seen one port. Thank you.

Mrs. MILLER. I thank the gentlelady very much.

The Chair recognizes the gentleman from Texas, Mr. Ratcliffe.

Mr. RATCLIFFE. Thank you, Chairman Miller and Ranking Member Vela, again, for the opportunity to be part of your subcommittee today and for holding this hearing on a critically important topic.

On the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, where I also serve, we talk a lot about cybersecurity threats to our power grids and to our nuclear missile silos and other critical infrastructure. But we, frankly, talk a lot less about the fact that 90 percent of the world's consumer goods are shipped on boats and vessels that come through our ports, and that statistic alone really underscores the gravity of the threat that we are talking about here. If the maritime industry suffered a major cyber attack, it could leave grocery store shelves empty. It could leave gas tanks at filling stations across the country empty, and, obviously, that would have a devastating, tremendous impact on our economy.

To that point, I want to ask about a report that was in the news last year—and maybe, Admiral Thomas, you may be the one to start with—I read a report that a U.S. port had suffered a 7-hour interruption of a GPS signal. Can you confirm that for me?

Admiral THOMAS. Yes. I mean, there's a container terminal that is fully automated that relies on GPS signal in order to locate specific containers and move cranes around. That particular disruption, if we are thinking about the same one, was ultimately determined not to be related to an intentional attack, but it does highlight the vulnerabilities associated with particularly relying on one system for that type of an operation.

Mr. RATCLIFFE. Terrific.

So given the challenges that the Department of Homeland Security and the Federal Government—I think it is well-known—are having in this arena with respect to the ability to retain a talented

and keep a talented cyber workforce, I would like to get your perspective.

There have been some discussions earlier about leveraging other resources, and within the Department, there is the NCCIC, the National Cybersecurity and Communications Integration Center. Is that a resource that you have been able to leverage? If not, why not, because a lot of what we have been talking about on the Homeland Security Committee generally is trying to elevate the NCCIC and its role and its use as a resource in this regard?

Admiral THOMAS. Well, I think you will be happy to hear that NCCIC is absolutely a resource for us, and as a resource, it impacts all three of our strategic priorities in our cyber strategy.

We have a Coast Guard person there full time. That is one of the ways we are building our own expertise, but it also ensures that NCCIC is fully linked up with our Coast Guard Cyber Security Operations Center. We are sharing information on a daily basis. We are taking information in from the industry, and we are providing information dozens and dozens of times a year to the industry on cyber threats, particularly in the maritime sector.

So NCCIC is every day getting more and more effective and getting more well-known and, I think, achieving their mission.

Mr. RATCLIFFE. Well, good. I am, actually, very pleased to hear that. So in follow-up to that, I would like to ask you, Mr. Parsons—because you talked a little bit about the information sharing aspect, and obviously, that is one of the things that the NCCIC tries to accomplish—has that been a resource for you, and, if not, why not?

Mr. PARSONS. In the Port of Long Beach, we have two cyber functions. We have two completely separate networks on the security side of the house. That is a reliance we have on the Enterprise Information Management Group. They have for the last 3 years had staffing, particularly as cybersecurity experts, and we looked at them to share that information on an enterprise level. With our stand-alone network, we share with various Federal databases. Both networks' personnel meet and talk with each other.

Both the Port of Los Angeles and the Port of Long Beach have CSOCs, a Cybersecurity Operations Center. The city of Los Angeles, the mayor's office, stood up a robust Cyber Fusion Center for the region, and both ports have connectivity with that.

I think part of the point you are trying to get to, though, is, to me, there is a lot of sharing going on, but I think there may need some better leadership and direction to make sure the right information is getting to the right people.

Mr. RATCLIFFE. Okay. Thank you.

Mr. Wilshusen, a follow-up because you, actually, you know, broached this subject and talked about some of the barriers to information sharing, but I assume that you're familiar with the bill that we moved through this committee and then successfully through the House, the National Cybersecurity Protection Advancement Act. That is an information sharing bill, and it does provide for—or intends to provide for, if passed into law, the opportunity to scrub out the type of information that has discouraged sharing personal identifying information, proprietary information, and to limit it to cyber threat indicators.

Any perspectives on that legislation, and was that what you were addressing?

Mr. WILSHUSEN. Well, I think, you know, to the extent that that legislation will improve the sharing of information on cyber threat incidents among the various different sectors and in the Federal agencies, it is going to be a positive. Indeed, you know, we are also going—we have been mandated—the GAO has been mandated to look at the NCCIC and how well it is implementing its mission roles and responsibilities in helping to facilitate the sharing of information.

Mr. RATCLIFFE. I appreciate you all being here today.

Again, I appreciate the opportunity to be on the subcommittee. I yield back.

Mrs. MILLER. I thank the gentleman.

I thank you both for attending. We appreciate it.

The gentleman from Texas.

Mr. VELA. Madam Chairman, I ask unanimous consent for the gentleman from Rhode Island, Mr. Langevin, to sit and question the witnesses at today's hearing.

Mrs. MILLER. Without objection, the Chair now recognizes Mr. Langevin, the gentleman from Rhode Island——

Mr. LANGEVIN. Thank you.

Mrs. MILLER [continuing]. A former Secretary of State as was myself.

Mr. LANGEVIN. Likewise. You bet.

I want to thank the witnesses for being here today.

Mr. Sawicki and Mr. Parsons, if I could just start with you.

Mr. Sawicki, one thing that caught my eye in your written testimony was your recommendation that DHS "further define and provide guidance on what constitutes a transportation security incident specific to potential or actual cyber breaches."

Can you and Mr. Parsons expand on this a bit further? What, if any, guidance have you received?

Mr. SAWICKI. Sure. Thank you very much for the question.

My recommendation is—the focus of it is to help understand that just because a facility is in a port and on the water, every security incident doesn't always elevate beyond the fence line to where it impacts the American transportation system. So I think it is important that we all come up with a—whatever that line is to where it is purely an internal crime versus something that needs to be reported through NRC and responded to by the Federal Government.

I am not aware of any specific guidance on what constitutes a transportation security incident based on cyber. I think in the majority of facility security plans or port security facility plans, there is always a question on what is a breach, what is a potential breach, and what is a near miss. So I think helping define that will help port facilities and ports report incidents that do occur.

Mr. LANGEVIN. So, can I ask you this? How do you report cybersecurity incidents to the Federal Government, and to whom have you reported?

Mr. SAWICKI. I think that is the question right now. We have not reported any cybersecurity incidents because we have not had any, that I am aware of, that are significant enough to report.

I think one thing to understand, specifically for the Port of Brownsville and many other mid-tier ports, that our focus right now is not so much protecting our networks through additional measures; it is upgrading semi-aging systems, so upgrading software, hardware that comes with the basic protections versus adding additional protections.

So, right now, if we were to have a breach to the port's cyber, to their internal email network, I think it would take some conversation to see who needs to be reported.

Mr. LANGEVIN. So let me take a different tack.

What incidents do you report, and what are the criteria you use to determine whether to report?

Mr. SAWICKI. Right now, our incidents that we report are breaches of security based on our facility's security plan—so somebody who may jump a fence, be seen jumping the fence, you know, who kind of breaks our perimeter—you know, the basic intrusion. If there is a threat that is reported, we will report that. But, right now, it is most of the reporting is done in accordance with our security plan and is based on an actual breach of our physical security.

Mr. LANGEVIN. So, right now, no criteria for reporting any type of a cyber event or intrusion?

Mr. SAWICKI. Correct.

Mr. LANGEVIN. Okay.

Mr. Parsons, if I could, in your testimony, you mentioned that ports can be reluctant to reveal they have been breached. Are there requirements as to what you must report?

Mr. PARSONS. No, sir, in the same vein about reporting. There is some confusion about what is reported to who. Our Information Management Division tells us we defend against approximately a million potential penetrations a day. That information is fed to the FBI's Cyberhood Watch Center. So they receive that information, and they analyze it with other reporting.

Should a major incident occur in the port complex, what we would do isn't any different than any other potential emergency situation. We would call the Coast Guard. We would call the FBI. We would call our partners. We would say, "Here's what we've got, where do you think this fits," because we have overlapping jurisdiction within maritime environments. So we work it out through personal communications and collaboration, but there isn't guidance to direct us.

Mr. LANGEVIN. Thank you, Mr. Parsons.

Admiral, if I could turn to you, Admiral Thomas.

How does the Coast Guard evaluate risk assessments and security plans with respect to cybersecurity, and have you found common challenges across different ports, and are there any model ports that you could point to in terms of protecting cybersecurity?

Admiral THOMAS. Well, thank you for the question.

If I could just take up the issue of reporting first.

I mean, we do receive reports of cybersecurity breaches in ports. We did receive one just last night, in fact. So there are reporting requirements. The cyber incidents that are related to the physical security requirements are reportable under the MTSA.

So, for example, if there is a loss of access control to a facility or a loss of cargo control or a loss of perimeter control that is associated with a cyber breach, that is a reportable incident.

The confusion comes because cyber touches all aspects of a port operation. So if it is a financial system, for example, that has been breached, well, that would not be reportable to the Coast Guard because it is not addressed under our authority. So I think the industry reps here are absolutely right that it is very confusing to figure out which type of incident gets reported to whom.

Now, for your question with regard to how do we address cyber risks in the ports, I mentioned earlier—I think before you entered the room—that we are working very closely across the interagency to develop those risk assessment tools so that what we employ in the maritime is consistent with what is employed in the power sector and in the financial sector, et cetera. There are a number of those tools under development—again, led by DHS—and we have piloted those in some of the major ports around the Nation.

There are definitely ports that have been more active—proactive, and it would be the ones that you would think about, those that have the larger amounts of really high-risk cargoes. Then there are others who are probably, rightly, just kind of waiting to see what develops in terms of standards.

Mr. LANGEVIN. Thank you. I see my time has expired, but I will have some follow-up questions. Perhaps, if you could respond for the record, I would appreciate it. Thank you.

Mrs. MILLER. I thank the gentleman very much.

The Chair now recognizes Ms. Jackson Lee from Texas.

Ms. JACKSON LEE. Madam Chair, could I yield to Mr. Donovan, and I will go last? I am still looking at my notes. Thank you.

Mrs. MILLER. Mr. Donovan has already had his 5 minutes. You are the last one.

Ms. JACKSON LEE. Then I cannot yield to Mr. Donovan, as they say.

Mr. DONOVAN. Thank you.

Ms. JACKSON LEE. Let me thank Mr. Vela and Mrs. Miller for this, and I am always glad to see the Brownsville Port here and acknowledge that Congressman Vela has done an excellent job in this capacity and has provided great leadership on these issues for the State of Texas.

Obviously, I am going to make note of the fact that we have the Houston Port, and we have a number of concerns about it.

So let me, first of all, ask Mr. Sawicki, are you aware of the FBI watch, and do you engage—use any Federal resources such as the FBI if you think something has occurred with respect to cybersecurity?

Mr. SAWICKI. Thank you very much.

I am aware of the FBI's InfraGard Program because I am a member of it, so I receive emails about current threats that, you know, can be sent out to people of my, I guess, stature, would be the best way to put it. So we coordinate the same way we coordinate cyber just like we coordinate safety and security in our ports. The Area Maritime Security Committees and Subcommittees are our primary method for information sharing and communication.

I have also worked in and throughout the Port of Houston and the Houston Ship Channel, and there it is the very same way. We have very robust Area Maritime Security Committees and very robust Harbor Safety Committees, and that is where a lot of that information sharing is happening.

Do we formally engage in Brownsville with the FBI currently? No, because there hasn't been the need to. We do—the topic does come up during AMSC meetings, but we have not—fortunately, we have not had a breach that would require us to coordinate with the FBI.

Ms. JACKSON LEE. What do you think the trepidation is for maritime companies not to share cyber attacks that have occurred?

Mr. SAWICKI. Competition. Competition and the potential for impact to their brand. We have seen some major breaches at some major companies, and we have seen CEOs lose their jobs. We have seen stock prices impacted. I think cyber is a little different because the likelihood of a cyber attack is as close to 100 percent as you can get. So I think private industry is protecting themselves because of that likelihood, and they are building crisis management programs around cyber just like they do around environmental issues and things like that. So private industry is working on it.

Ms. JACKSON LEE. We understand that a decade or so ago, this committee established that over 85 percent of the infrastructure which would be subject to many attacks was in the private sector, and we have started to send out messages for them to prepare.

But what can the Federal Government do that you think would be effective in sort of easing the concern of competition and looking more closely at the vast massive impact that would come from a cyber attack and particularly at the port?

Mr. SAWICKI. I think, initially and what is happening right now, it is facilitating the conversation, but ultimately, it is ensuring that any data that is shared is protected. So protecting your own networks first while private industry works to protect their networks and then to help—to continue funding training programs. You know, like I said, many ports right now are not the very large—not the Port of Houston, not the Port of Long Beach—to where the need is training. You know, we can have all the systems in the world, but if I click the wrong email, it can get right around all of it.

So I think facilitating training, continuing to support the Port Security Grant Program, and then really looking at some of the cost-mass requirements for cyber projects that could potentially mitigate risk at a National level.

Ms. JACKSON LEE. Thank you.

Admiral Thomas, I can't see you, but I know, by your excellent answers, that you are here.

Let me have a series of questions with you, albeit briefly then. I thank the Chairman.

As I do that, let me acknowledge the Brownsville Port, but then, of course, I have in my jurisdiction the Houston Port, which is a 25-mile-long complex of diversified public and private facilities and is a few hours away from Gulf of Mexico, which makes it vulnerable on a number of occasions—on number of points: It is manmade. It has major exports. In 2012, Ship Channel-related busi-

nesses contributed 1 million-plus jobs and 178 plus 5 billion in State-wide economic activity.

You heard the gentleman from the Port of Brownsville about competition and what could be done. You see the difference in size of the many ports across America.

In terms of the Coast Guard's cybersecurity effort, how does the present structure of sequester impact that, and what answer would you give to the private sector who would be willing to give more information if they could be assured of the lack of a breach? What are the firewalls that we are putting in place or have in place?

Admiral THOMAS. Well, thank you for the question.

With regard to the impact of sequester on our cyber operations, particularly our efforts to secure the critical infrastructure, I would say it is minimal now because we are still in the assessing and communicating phase, in the process of figuring out, what are the proper performance standards to put into place? As we move into a phase where we actually have to ensure compliance with those standards, then I think the resource demands become heavier on us.

Ms. JACKSON LEE. What is your projection for moving up to the next step?

Admiral THOMAS. Well, one of the interesting things about this cyber question is that it is not really uniquely maritime in that what we do in the maritime really needs to be closely aligned with and look a lot like what goes on in other sectors, so I think the Government needs to move through this.

In other words, I don't think we want to be implementing hard standards in the maritime ahead of many of the other sectors, particularly those sectors that this—the maritime ports connect with because you wouldn't want to put in place separate requirements for entities that—you know, my rail is going to have to meet this, and my port facilities are going to have to meet that, and my trucking facilities something else.

So I don't know. I think that the time line, though, has to be carefully coordinated and considered.

Ms. JACKSON LEE. Is that the Government's challenge to coordinate the private sector and cybersecurity, because maybe, Admiral, you might have a best practices idea under the Coast Guard that might be utilized by the railroads and otherwise? I am trying to see who starts, and what would be most helpful to get us into this process as I conclude.

Admiral THOMAS. So DHS really has taken a leadership role in coordinating across all the sectors, and the Coast Guard participates in that as does the TSA and all the other sector-specific agencies. So I think the focus on sharing those best practices across sectors—and certain sectors are leading, financial, for example, and energy—is definitely in place, and the private sector is very involved in that effort.

Ms. JACKSON LEE. Thank you, Madam Chair.

Mrs. MILLER. I thank the gentlelady. I appreciate it.

Ms. JACKSON LEE. If I——

Mrs. MILLER. I am going to move on here. We have a hard deadline.

Ms. JACKSON LEE. I understand. When the gentleman finishes, I just want to put a "thank you" on the record.

Mrs. MILLER. Certainly.

Ms. JACKSON LEE. So I would appreciate it.

Mrs. MILLER. The Chair recognizes the gentleman from Texas now, Mr. Hurd.

Mr. HURD. Thank you, Madam Chairman.

Thank you all for being here today.

This question is directed at any one of you all that want to field it, and I want to pick up on some of the questions that my colleague from Houston has talked about.

You know, ports, like many other industries in the world, are moving towards automation, integration, you know, and upgrades to industrial control systems. You know, probably the two publicly-known cases of physical damage occurring as a result of a cyber attack is Stuxnet, probably being the most well-known, and it occurred as a result of cyber attacks against industrial control systems.

You all have talked about information sharing, but what are some of the unique challenges you all are dealing with in protecting industrial control systems, and, you know, what are you all doing specifically in that area?

The admiral, maybe, or Mr. Parsons.

Admiral THOMAS. Well, I mean, I can talk to you about what I know is going on in some of the higher-tech portions of the maritime industry.

So, for example, those vessels that are out in the Gulf of Mexico, drilling in very, very deep water, relying on dynamic positioning systems and systems that are making decisions faster than people can humanly make them, which enables them to drill, you know, miles down—that they really have begun to focus—rightly, I believe—on what I call a layered cyber protection strategy, which starts with individual components, the manufacturers of those components, how those are made, how they have been integrated into a system, and how that system is then integrated on the vessel but then, beyond that, really focusing on the human elements because this is more than just an IT problem.

Also, how are those systems operated and maintained, and how are the operators and maintainers trained, because very basic training, like don't plug your iPhone into this system, can go a long way to help to prevent?

So what I have seen, particularly in those portions of industry that rely more heavily on high-tech, is a risk-management approach for cyber that is akin to what they have always done for physical threats, and I think that is a positive step.

Mr. WILSHUSEN. I would just add, too, that one of the key elements to the increasing use of industrial control systems that have communications capability is just making sure that entities and corporations are aware of that capability and the threats associated with that.

What we had found in a couple of our reviews is that the agency—and this is going back a few years—was not even familiar or did not know that its industrial control systems were actually con-

nected to the administrative networks of the organization, and that created another avenue of access, if you will.

So understanding the threats to the technologies that are being used and how that technology is being used is going to be key to that, particularly as it relates to industrial control systems.

Mr. HURD. I yield my final 2 minutes to my colleague from Texas. Thank you.

Ms. JACKSON LEE. Thank you, Mr. Hurd.

I wanted to just say to the admiral but pose a question as well, first of all, thank you for the stunning and—obviously, I know you will say they were doing their duty work regarding the cargo ship off the coast of Florida during a very horrific time. I don't know if the Chairman and Ranking Member know of the interests that I have because I think security involves many aspects of our work, and that—we have no evidence of anything untoward. But certainly it was a tragic episode and a loss of life of many Americans.

So, Admiral, I am thankful to you, and the question that I have that you could either do in writing—or I think I have a few minutes for you to answer—is: Any directions—or does the company and/or the captain seek information from the Coast Guard, their communications on-going that might draw the attention to come back to harbor in any situations like that?

Admiral THOMAS. Well, as you know, our investigation of that particular casualty is just starting under the lead of the NTSB, and those questions will certainly be asked. It is really the human element: What information was looked at by whom and when? Generally, though, a master of a ship of that size is not consulting with the Coast Guard with regard to his or her voyage planning.

Ms. JACKSON LEE. Is not consulting?

Admiral THOMAS. Is not consulting with the Coast Guard with regards to their voyage planning. Obviously, they are required to let us know when they tend to make a port call, but the voyage planning is something that is left to the ship's master and the company.

But, as I said, our investigation with the NTSB will look into all of those factors, and we will be in a better position to let you know the specifics, hopefully in a few weeks.

Ms. JACKSON LEE. Thank you.

Mrs. MILLER. Thank you.

Ms. JACKSON LEE. Thank you, Mr. Hurd.

Mrs. MILLER. We thank the gentlelady for those comments.

We began our meeting, actually—our hearing—by thanking the coastguardsmen and women for their extraordinary service in that incident.

Thoughts and prayers, obviously, to all the families, the people that have been lost.

So I want to thank the witnesses—all of you—for joining us today. I think it has been a very good hearing, a very timely subject, one that is not going away. It is something that we have to pay an incredible amount of attention to.

So the Members of the committee might have some additional questions for the witnesses, and I would ask you all to respond to those in writing if they do put those in writing.

Pursuant to the committee rule 7(e), the hearing record will be held open for 10 days.

Without objection, thank you all again for attending.

The committee stands adjourned.

[Whereupon, at 11:30 a.m., the subcommittee was adjourned.]

○