OCTOBER 8, 2015

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

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

ONE HUNDRED FOURTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

MEMBER STATEMENTS:

Rep. Candice Miller (R-MI) *[view pdf]*
Chairman, Subcommittee on Border and Maritime Security

Rep. Filemon Vela, Jr. (D-TX) *pdf unavailable; 7:35 of hearing webcast*
Ranking Member, Subcommittee on Border and Maritime Security

WITNESSES:

RDML Paul F. Thomas (USCG) *[view pdf]*
Assistant Commandant for Prevention Policy, United States Coast Guard

Mr. Gregory C. Wilshusen *[view pdf]*
Director, Information Security Issues, U.S. Government Accountability Office

Mr. Randy D. Parsons *[view pdf]*
Director, Security Services, Port of Long Beach, CA

Mr. Jonathan Sawicki *[view pdf]*
Security Improvement Program Manager, Ports of Brownsville and Harlingen, TX

This hearing compilation was prepared by the Homeland Security Digital Library, Naval Postgraduate School, Center for Homeland Defense and Security.

AVAILABLE WEBCAST(S):*

Full Hearing: *https://youtu.be/u05frVPza8c*

COMPILED FROM:

https://homeland.house.gov/hearing/protecting-maritime-facilities-in-the-21st-century-are-our-nations-ports-at-risk-for-a-cyber-attack/

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

HOMELAND SECURITY
COMMITTEE

OPENING STATEMENT
October 8, 2015

MEDIA CONTACTS
Susan Phalen, Matthew Ballard

Statement of Subcommittee Chairman Candice Miller (R-MI)
Border and Maritime Security Subcommittee
House Homeland Security Committee

Protecting Maritime Facilities in the 21st Century: Are Our Nation's Ports at Risk for a Cyber-Attack

Remarks as Prepared

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 cyber security 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 cyber security 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 automation 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 cyber security 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 nationwide. 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 cyber security standards? I think there is merit in looking at that model for cyber security 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.

###

U. S. Department of
Homeland Security

United States
Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-0921
Phone: (202) 372-3500
FAX: (202) 372-2311

TESTIMONY OF
REAR ADMIRAL PAUL F. THOMAS
ASSISTANT COMMANDANT FOR PREVENTION POLICY

ON
CYBERSECURITY IN U. S. PORTS

BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY
BORDER & MARITIME SECURITY SUBCOMMITTEE

8 OCTOBER 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 approach 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 cyberspace, 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 U.S., 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' 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 sub-committees, 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.

United States Government Accountability Office

Testimony
Before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, October 8, 2015

MARITIME CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Enhance Efforts to Address Port Cybersecurity

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

GAO Highlights

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

October 8, 2015

MARITIME CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Enhance Efforts to Address Port Cybersecurity

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.

View GAO-16-116T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

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

[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, D.C.: Feb. 11, 2015).

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

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

- 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 nonfederal 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

[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).

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 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 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

[6] GAO-14-459.

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 nonfederal 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 nonfederal 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 one 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 nonfederal 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.

Contact and Acknowledgments

If you or your staff have any questions about this testimony, please contact Gregory C. Wilshusen, Director, Information Security Issues at (202) 512-6244 or wilshuseng@gao.gov. GAO staff who made key contributions to this testimony are Michael W. Gilmore, Assistant Director; Bradley W. Becker; Jennifer L. Bryant; Kush K. Malhotra; and Lee McCracken.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.

The Port of
LONG BEACH

The Written Statement of

Randy Parsons

Director of Security Services

Port of Long Beach

Before the

House Committee on Homeland Security

Subcommittee on Border and Maritime Security

United States Congress

"Protecting Maritime Facilities in the 21st Century: Are Our Nation's Ports At Risk For A Cyber Attack?"

October 8, 2015

Port of Long Beach
1249 Pier F Avenue
Long Beach, CA 90802
(562) 283-7814

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 twenty-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.

Cyber Security

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, cyber security 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 one 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 manmade 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 11th 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 11th attacks.

It may seem overdramatic to make a comparison to the September 11th attacks, but one similarity may be in the number of cyberattacks that have taken place internationally and within the U.S., as well as our responses, or lack of, to those warnings. As a result, business resiliency has become a critical part of our ongoing 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 manmade) and continue to provide an acceptable level of goods movement. In order to develop a comprehensive resiliency plan to address cyber security, factors that should be addressed include infrastructure needs and protection, transportation systems, and development of business continuity plans.

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 patch work 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 cyber security 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 cyber security 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 cyber security activities by placing emphasis within the Port Security Grant Program (PSGP) on grant applications that focus on cybersecurity mitigation. It is important that cyber security 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 cyber security 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 cyber security 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 Cyber Security 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 cyber security 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 three 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, multiagency, 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 cyber security 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 cyber security–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 roadmap 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.

TESTIMONY OF
MR. JONATHAN SAWICKI
SECURITY IMPROVEMENT PROGRAM MANAGER
THE PORTS OF HARLINGEN AND BROWNSVILLE, TEXAS

ON
CYBERSECURITY IN U. S. PORTS

BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY
BORDER & MARITIME SECURITY SUBCOMMITTEE

8 OCTOBER 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 cyber security 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 worldwide 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 FY2015 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 Cyber Security Strategy

In general I support the USCG's vision for operating in the cyber domain, and the three primary priorities of defending cyberspace, 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 ongoing 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 cyberspace 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 cyber security 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 ongoing 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.