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.