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.