Foreign Policy
at BROOKINGS

The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities

Commander Joseph Kramek,
United States Coast Guard
FEDERAL EXECUTIVE FELLOW

CENTER FOR 21st CENTURY SECURITY AND INTELLIGENCE

POLICY PAPER
July 2013

Foreign Policy
at BROOKINGS

The views expressed in this monograph are those of the author and do not reflect the official policy or position of the United States Coast Guard, Department of Homeland Security, Department of Defense, or the U.S. Government.

COVER PHOTO COURTESY OF THE U.S. COAST GUARD FLICKR

CONTENTS

ILLUSTRATIONS

EXECUTIVE SUMMARY

"America must also face the rapidly growing threat from cyber-attacks . . . our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."[1] *-- President Barack Obama, 2013 State of the Union Address*

Today, U.S. port facilities rely as much upon networked computer and control systems as they do upon stevedores to ensure the flow of maritime commerce that the economy, homeland, and national security depend upon. Yet, unlike other sectors of critical infrastructure, little attention has been paid to the networked systems that undergird port operations. No cybersecurity standards have been promulgated for U.S. ports, nor has the U.S. Coast Guard, the lead federal agency for maritime security, been granted cybersecurity authorities to regulate ports or other areas of maritime critical infrastructure. In the midst of this lacuna of authority is a sobering fact: according to the most recent National Intelligence Estimate (NIE) the next terrorist attack on U.S. Critical Infrastructure and Key Resources (CIKR) is just as likely to be a cyber attack as a kinetic attack.[2]

The potential consequences of even a minimal disruption of the flow of goods in U.S. ports would be high. The zero-inventory, just-in-time delivery system that sustains the flow of U.S. commerce would grind to a halt in a matter of days; shelves at grocery stores and gas tanks at service stations would run empty. In certain ports, a cyber disruption affecting energy supplies would likely send not just a ripple but a shockwave through the U.S. and even global economy.

Given the current absence of standards and authorities, this paper explores the current state of cybersecurity awareness and culture in selected U.S. port facilities. The use of the post-9/11 Port Security Grant Program (PSGP), administered by the Federal Emergency Management Agency in consultation with the Coast Guard, is also examined to see whether these monies are being used to fund cybersecurity projects.

In the end, the research shows that the level of cybersecurity awareness and culture in U.S. port facilities is relatively low. In most ports, basic cybersecurity hygiene measures are not being practiced. Of the ports studied, only one had conducted a cybersecurity vulnerability assessment, and not a single one had developed a cyber incident response plan.

PSGP federal program managers have not expressly included cybersecurity projects in their funding criteria. While this did not exclude ports from seeking PSGP monies for cybersecurity projects, it certainly did not incentivize them. Of the $2.6 billion allocated to the PSGP over the past decade, less than $6 million—or *less than one percent*—was awarded for cybersecurity projects, and only one port in this study had used PSGP monies for a cybersecurity project. Ironically, a large number of security systems purchased with PSGP monies are networked into port command centers, making them more vulnerable to cyber attacks.

Most municipal ports are so-called landlord ports that lease out their terminals to private entities. Thus, the research also found that landlord ports have little awareness of what networked systems are being run by their lessees and almost no awareness of what, if any, cybersecurity measures are being taken to protect these systems.

Based on these findings, a series of policy recommendations are provided for Congress, DHS and the Coast Guard, and port facility owners and operators for how cybersecurity in U.S. port facilities might be incentivized and improved. In sum, these recommendations call for: Congress to pass legislation that provides the Coast Guard authority to enforce cybersecurity standards for maritime critical infrastructure (consistent with how it already enforces physical security in maritime critical infrastructure); the adoption of NIST cybersecurity standards for port facilities; DHS to structure the PSGP grant program to incentivize cybersecurity projects; the Coast Guard to ensure a functional information sharing network is in place that allows government, port owners and operators, and maritime industry stakeholders to exchange cyber threat information; and port owners and operators to conduct cyber vulnerability assessments and prepare response plans. *Most of these recommendations are relatively simple steps that will greatly enhance not only maritime cybersecurity and resilience but ultimately U.S. homeland and national security.*

Notes

[1] Barack Obama, "2013 State of the Union Address," speech given at U.S. Capitol, Washington, DC, February 4, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address.

[2] Ellen Nakashima, "U.S. said to be target of massive cyber-espionage campaign," *The Washington Post*, February 11, 2013, pp. A-1, 11, http://articles.washingtonpost.com/2013-02-10/world/37026024_1_cyber-espionage-national-counterintelligence-executive-trade-secrets.

CHAPTER ONE

Introduction: Why "Maritime" Cybersecurity?

The United States is widely recognized as one of the world's leading digital and cyber economies.[1] Goods can be ordered over the Internet in seconds, and they ship out just minutes later. However, what is less recognized is that most of these goods are still carried as they have been for centuries—by sea.[2] More than 95 percent of this trade is handled by U.S. seaports.[3] While the U.S. may be a leader in e-commerce, it very much remains a maritime nation. This is why since its earliest days U.S. economic prosperity has been dependent upon maritime security. International maritime trade exceeds 30 percent of the U.S. global domestic product, and this value is only expected to increase.[4] In 2011, over 9,000 individual vessels, from 85 different Flag Administrations, made almost 80,000 port calls to the United States' 361 ports.[5] U.S. national security is also dependent upon maritime security. When the U.S. military is called into action, much of its equipment ships out of U.S. military outload ports that comprise the National Port Readiness Network.[6] Indeed, almost 50 percent of the supplies for the U.S. military's operations in Afghanistan and Iraq shipped through a single U.S. port—the Port of Beaumont, Texas.[7]

While the U.S. reliance on secure maritime trade has not changed over the course of two centuries, what has changed dramatically is how maritime commerce is controlled and managed. Today, ports rely as much on computer networks as on human stevedores. Complex networked logistics management systems undergird the global flow of maritime commerce. These systems track maritime cargo from the time a container is stuffed by a merchant overseas until it reaches its final destination at a U.S. retailer. They are so sophisticated they have essentially done away with the warehouse; today, goods are "stored in transit." Networked control systems are also often involved in the loading and unloading of these goods. Modern gantry cranes and other systems use optical recognition and other technologies to locate, scan, and manage all facets of port terminal operations. Port facilities often leverage information from these same systems to comply with security requirements. Scanners and radio frequency identification devices (RFID) not only track cargo as it enters or exits ports, they also track the trucks, railcars, and drivers that operate these conveyances.

Yet the maritime industry has paid little attention to the security of these networks. In November 2011, the European Network and Information Security Agency (ENISA) reported that, "[t]he awareness on cybersecurity needs in the maritime sector is currently low to non-existent."[8] This research, which focused on U.S. port facilities,

found awareness of cybersecurity needs in a similar state. *Of the six ports studied, only one had conducted a cybersecurity vulnerability assessment and not a single one had a cyber incident response plan. Moreover, of the $2.6 billion allocated to the U.S. Port Security Grant Program – created in the wake of 9/11 to fund new congressionally mandated security requirements at U.S. ports – to date, less than $6 million has been awarded for cybersecurity projects.*

What would the potential consequences be if a hacker sought to disrupt the flow of goods in U.S. ports? *The zero-inventory just-in-time delivery system that sustains the flow of U.S. commerce would grind to a halt in a matter of days; shelves at grocery stores and gas tanks at service stations would run empty.* Indeed, we have several real-life examples of how this might occur. The November 2012 impact of Hurricane Sandy caused severe damage in the Ports of New York and New Jersey, preventing shipments of petroleum from being offloaded and trucked from ports to filling stations.[9] Tanks at gas stations across the region quickly ran dry. In just days, residents relying on gasoline generators for heat and power began to panic. In another incident in 2012, labor strikes in the Port of Los Angeles-Long Beach forced ships to remain offshore, shutting down terminal operations, and causing truckers and rail cars to back up outside port entrances, resulting in an economic impact of $1 billion per day in lost wages, business revenue, and the value of cargo that had to be diverted to other ports.[10] It is fair to assume that a cyber attack on U.S. maritime critical infrastructure would disrupt port operations to a similar, if not worse degree. Indeed, a range of possible cyber threats exist—from less sophisticated actors engaged in criminal activity and criminal hacking groups attempting to carry out acts of disruption and terrorism, to the extreme end of the spectrum that includes acts of war by belligerent nation states.[11]

U.S. port facilities are so vital to U.S. economic and national security that the Department of Homeland Security has identified them as one of only 16 designated sectors of U.S. Critical Infrastructure (CIKR).[12] *However, while fledgling efforts are underway, no cybersecurity standards currently exist for U.S. port facilities.*[13] *And, even if they did, the agency assigned responsibility for the security of U.S. maritime critical infrastructure – the United States Coast Guard – does not have specific authority to regulate cybersecurity in port facilities or any other area of maritime critical infrastructure.*[14]

The Coast Guard's current port security authorities empower them to enforce the physical security provisions required by the Maritime Transportation Security Act (MTSA)—a statute passed in the wake of the 9/11 attacks that was designed to protect U.S. maritime critical infrastructure against kinetic terrorist attacks.[15] MTSA does not contain any cybersecurity requirements, nor do any of the 13 major regulations predicated upon it.[16] *Rather, MTSA's requirements can loosely be summed up as guns, gates, guards, and identification cards.* Since the Coast Guard focuses on holding port facilities accountable for compliance with MTSA's physical security requirements, it is no

surprise that port facility owners and operators also focus on physical security and not cybersecurity.

In the midst of this lacuna of authority is a sobering fact: according to the most recent National Intelligence Estimate (NIE) the next terrorist attack on U.S. critical infrastructure is just as likely to be a cyber attack as a kinetic attack.[17] The fact that The White House released an Executive Order and Presidential Policy document directing U.S. government agencies to take steps to seek voluntary cooperation from private industry to protect U.S. CIKR when Congress failed to pass cybersecurity legislation is further evidence of the seriousness with which the administration views a cyber attack on U.S. CIKR. However, it remains to be seen whether these executive directives, which depend upon the private sector to voluntarily share proprietary information with government agencies and thus lack the teeth of legislation, will provide a sufficiently robust framework to protect against this emerging and dynamic threat.

Notwithstanding the current lack of standards and enforcement authorities, port facility owners, operators, and the maritime industry are certainly able to take independent actions to protect the networks and systems upon which their operations rely. The question is, have they? Moreover, are they incentivized to do so? Thus, this research seeks to understand the current state of cybersecurity awareness and culture in U.S. port facilities. What, if any, independent efforts are being made to protect port facilities upon which the U.S. economy, U.S. homeland, and U.S. national security are so dependent? Do larger port facilities have a leg up on smaller facilities, perhaps because of the significant grant monies they receive? Are there best and most promising practices that can be replicated? And, going forward, how can we strengthen U.S. port facilities against the threat of cyber attack to ensure U.S. maritime critical infrastructure is sufficiently resilient and to guarantee rapid recovery from a cyber attack?

Notes

[1] "Research and Markets: Global B2C E-Commerce Trends Report 2013," *The Wall Street Journal*, April 30, 2013, http://online.wsj.com/article/PR-CO-20130430-911280.html.

[2] U.S. Department of Transportation, "U.S. Water Transportation Statistical Snapshot," Maritime Administration, February 2011, http://www.marad.dot.gov/library_landing_page/data_and_statistics/Data_and_Statistics.htm.

[3] U.S. seaports are responsible for moving nearly all of the country's overseas cargo volume, 99.4 percent by weight and 64.1 percent by value. *See* American Association of Port Authorities, "Seaports and the U.S. Economy," http://aapa.files.cms-plus.com/PDFs/Awareness/US%20Economy%20Fact%20Sheet%2012-4-12.pdf, accessed April 2013.

[4] Ibid. International Trade via seaports accounts for more than 32 percent of the U.S. GDP; that value is expected to increase to the equivalent of 37 percent by 2015 and 60 percent by 2030.

[5] U.S Department of Homeland Security, "Written testimony of U.S. Coast Guard Assistant Commandant for Prevention Policy Rear Admiral Joseph Servidio for a House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation hearing

titled "Tenth Anniversary of the Maritime Transportation Security Act: Are We Safer?" September 11, 2012, http://www.dhs.gov/news/2012/09/11/written-testimony-us-coast-guard-house-transportation-and-infrastructure.

[6] Headed by the Maritime Administration, ten federal agencies and organizations provide coordination and cooperation to ensure readiness of designated commercial ports to support deployments during contingencies and defense emergencies. *See* U.S. Department of Transportation, "National Port Readiness Network (NPRN)," Maritime Administration, http://www.marad.dot.gov/ports_landing_page/nprn_home/nprn_home.htm, accessed April 2013.

[7] Port of Beaumont, http://www.portofbeaumont.com/, accessed April 2013.

[8] European Network and Information Security Agency, "Analysis of Cyber Security Aspects in the Maritime Sector," November 2011, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts/cyber-security-aspects-in-the-maritime-sector-1.

[9] Kate Zernike, "Gasoline Runs Short, Adding Woes to Storm Recovery," *The New York Times*, November 1, 2012, http://www.nytimes.com/2012/11/02/nyregion/gasoline-shortages-disrupting-recovery-from-hurricane.html?pagewanted=all&_r=0.

[10] Ronald White, "Port Labor Talks Shift into High Gear, but Strike Continues," *Los Angeles Time*s, December 1, 2012, http://articles.latimes.com/2012/dec/01/business/la-fi-mo-ports-strike-continues-20121201.

[11] Barack Obama, "Improving Critical Infrastructure Cybersecurity," Executive Order, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

"Critical Infrastructure Security and Resilience," Presidential Policy Directive/PPD-21, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[12] The sixteen critical infrastructure sectors are: 1) Chemical, 2) Commercial Facilities, 3) Communications, 4) Critical Manufacturing, 5) Dams, 6) Defense Industrial Base, 7) Emergency Services, 8) Energy, 9) Financial Services, 10) Food and Agriculture, 11) Government Facilities, 12) Healthcare and Public Health, 13) Information Technology, 14) Nuclear Reactors, Materials and Waste, 15) Transportation Systems, and 16) Water and Wastewater Systems. *See* Presidential Policy Directive/PPD-21 and DHS list of Critical Infrastructure Sectors at http://www.dhs.gov/critical-infrastructure-sectors.

[13] National Institute for Standards and Technology Information Technology Laboratory, "Cybersecurity Framework," http://www.nist.gov/itl/cyberframework.cfm, accessed May 2013.

The U.S. Coast Guard also has established a page on its website that details its participation in the NIST-led cybersecurity framework development process. *See* Homeport, "Cybersecurity," U.S. Department of Homeland Security, https://homeport.uscg.mil/mycg/portal/ep/channelView.do?channelId=-54883&channelPage=%2Fep%2Fchannel%2Fdefault.jsp&pageTypeId=13489&BV_SessionID=@@@@1184155535.1369077996@@@@&BV_EngineID=cccdadfjllmlgfdcfngcfkmdfhfdfgm.0, accessed May 2013.

[14] Presidential Policy Directive – Critical Infrastructure Security and Resilience/PPD-21 designates the Co-Sector Specific Agencies for the Transportation Sector as the Department of Homeland Security and the Department of Transportation. DHS has designated its component agency, the U.S. Coast Guard, as the lead agency for Maritime Critical Infrastructure (MCI). SSAs are the federal departments or agencies responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. PPD-21 expressly revoked prior policy guidance contained in DHS Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection (HSPD-7), however, plans developed pursuant to HSPD-7 remain in effect until specifically revoked or suspended.

[15] MTSA was codified into U.S. law as Chapter 701, Port Security, of title 46, United States Code. MTSA was subsequently amended by the Security and Accountability For Every (SAFE) Port Act of 2006 (P.L. 109-347) and the Coast Guard Authorization Act of 2010 (P.L. 111-281).

[16] The Coast Guard has since issued 13 major maritime security regulations. Examples include: Advanced Notice of Arrival (ANOA) requirements (requiring large commercial vessels bound for U.S. ports to send a message 96 hours prior to arrival with details concerning their vessel, cargo, crew and last ports of call); Vessel Security Requirements; Facility Security Requirements; Long Range Identification and Tracking of Ships (LRIT); Automatic Identification Systems (AIS); and Crewmember Identification requirements, to name a few. *See*, 33 C.F.R. 101, Subchapter H.

[17] Ellen Nakashima, "U.S. said to be target of massive cyber-espionage campaign," *The Washington Post*, February 11, 2013, pp. A-1, 11, http://articles.washingtonpost.com/2013-02-10/world/37026024_1_cyber-espionage-national-counterintelligence-executive-trade-secrets.

CHAPTER TWO
Methods and Background

Methods

Using an interview and visit case-study approach, the author visited port facilities and interviewed port security officials, government officials, and other stakeholders in person or by phone. A diverse constellation of port facilities was purposefully selected, based upon their threat ranking by DHS, their size, volume of cargo, type of cargo (containers, military, petroleum), and geographic location (East Coast, West Coast, Gulf Coast, Inland). The ports chosen include:

- The Port of Baltimore, MD
- The Port of Houston, TX
- The Port of Los Angeles, CA
- The Port of Long Beach, CA
- The Port of Vicksburg, MS
- The Port of Beaumont, TX

The rest of this chapter will provide background on the current port security authorities and practices. In chapter three, we explore the six ports examined in this research. Chapter four will further aggregate the collected data and organize the findings under the following criteria: 1) Awareness; 2) Prevention and Preparedness; and, 3) Response and Recovery. And the final chapter will provide recommendations for action to Congress, DHS and Port Security Grant Program administrators, the Coast Guard, and port facility owners, operators, and security officers.

Background

U.S. Port Ownership and Administration

Some background on U.S. ports and how they are administered is required to understand both this research and the complex challenge of cybersecurity in U.S. port facilities.

There is an old saying among Coast Guard port inspectors, "If you've seen one port, you've seen one port." But while each port has certain unique aspects, there are some patterns.

Many major U.S. port facilities are sited on property owned by a governmental entity and operated by port authorities. However, the majority of U.S. terminals are privately owned, making port security a joint public-private endeavor.[1] Public ports are normally owned by a state, a municipality, or in some cases a specially created subdivision of government sometimes referred to as a "navigation district" or "harbor district" that allows the government entity to conduct business as a quasi-private entity.[2] Thus, the personnel overseeing these ports' operations are state or municipal government employees. They are typically organized under a director, who is selected by a group of port commissioners. The commissioners carry out an oversight role, similar to that of a board of directors, and report to the head of government, normally the state governor or mayor of the municipality. In contrast, the personnel who perform the ports' hard work of loading and unloading vessels, including stevedores and longshoreman, along with many other required trades, are almost exclusively members of organized labor unions that have master and local contracts with port terminals, the most prominent being the 65,000 member International Longshoremen's Association, AFL-CIO.[3]

Ports are extremely important to the government entities that operate them for three reasons: 1) ports are a major source of direct and indirect employment in their local economies; 2) the fees from port operations generate large direct and tax revenue streams for its owners; 3) population centers including the nation's largest cities have naturally formed around ports, ensuring their interest in keeping the ports' flow of commerce uninterrupted and ensuring the safety of these high population density areas. However, the manner in which government entities administer their ports varies greatly. A typical port has several terminals or lay berths—docks where ships can moor and offload their goods and passengers. Some ports choose to simply lease out their terminals and remove themselves from operations. These are referred to as "Landlord Ports." Even though Landlord Ports are not engaged in the business of offloading and onloading goods, they are still normally responsible for providing security and utilities, and they also must comply with federal security regulations like MTSA. Private entities, whether they lease a terminal from a Landlord Port or own the terminal, are also subject to federal security regulations including MTSA.

Alternatively, government entities that choose to engage in port facility operations are known as "Operating Ports." As *both* owners and operators, Operating Ports typically have more visibility on the operations within their facilities. They are also directly subject to compliance with the full spectrum of MTSA's facility regulations. Some government entities choose to directly operate some of their port terminals while leasing others. These are referred to as "Limited Operating Ports" or "Hybrid Ports." What remain are the private maritime entities that own or lease maritime facilities, to include a myriad of national, international, foreign, and multinational corporations. The one constant is that every facility operator, whether it's a Landlord, Operating,

Limited Operating or private port facility, is required to comply with the applicable portions of MTSA's security requirements.

Port Security– Pre and Post-9/11 and the Maritime Transportation Security Act

The complex ecosystem of port authorities and those who operate them is what makes port security such a challenging and sometimes vexing charge for both facility operators and the agencies responsible for regulating them. The U.S. Coast Guard has regional commands called "Sectors" that are typically collocated near major U.S. port areas. Coast Guard Sector Commands are, among other things, tasked with the responsibility of inspecting port facilities and ensuring their facility security measures are in compliance with MTSA's regulations. Coast Guard port facility inspectors typically strive to conduct one pre-scheduled inspection and one unscheduled inspection at every facility within their jurisdiction each year. To be clear, this means that within our nation's 361 port the U.S. Coast Guard must inspect some 3,200 cargo and passenger handling facilities to ensure their "guns, gates, guards and identification cards" comply with MTSA regulations.

MTSA and its corresponding regulations were tailored to protect U.S. ports and waterways from a kinetic terrorist attack.[4] MTSA requires, among other things, threat and security assessments on port facilities and vessels. Vessel and facility security plans must contain passenger, vehicle and baggage screening procedures, security patrols, personnel identification procedures, and physical security measures including access controls and surveillance cameras. U.S. Coast Guard inspectors also visit some 2,500 foreign ports to verify that they have effective security plans.

MTSA also authorized the creation of Area Maritime Security Committees (AMSC). The AMSC serves as a forum for port stakeholders, including federal, state, and local agencies, as well as private industry representatives. The AMSC also develops the port's Area Maritime Security Plan (AMSP). *There are currently 43 AMSCs*. They typically hold monthly meetings, share information, and coordinate activities. The AMSCs are as unique as their ports, but they have evolved into a very productive, powerful, and popular entity in U.S. ports. Simply put, today the AMSCs are where the business of port security gets done.

Of particular note for the issues of technology gains and vulnerabilities, MTSA has also required a new identification credential – the Transportation Worker Identification Care (TWIC) – for all persons working within ports, including longshoreman, truckers, seaman, and all other categories of workers. TWIC cards are designed to be read by electronic readers and contain unique features that pair the cardholder to the card (to ensure use only by its unique cardholder). Persons having

business in ports who do not hold TWIC cards, such as seaman aboard visiting ships, must be escorted if they enter the port for any reason. The TWIC program experienced significant technological challenges in implementation as well as pushback from truckers and merchant mariners who were already required to maintain other credentials such as merchant mariner licenses and commercial driver's licenses. Today, ports are still struggling with purchasing approved electronic TWIC card readers and the technology—much of it networked—to implement them.[5]

The Port Security Grant Program (PSGP)

To assist ports in funding many of MTSA's new security requirements, MTSA codified the Port Security Grant Program (PSGP).[6] Since the PSGP's inception, more than $2.6 billion has been appropriated.

Today, the Federal Emergency Management Agency (FEMA), a component agency of DHS, has responsibility for administering the PSGP.[7] Since the U.S. Coast Guard is the lead agency for port security, FEMA consults with the Coast Guard to leverage its maritime expertise, along with other maritime agencies and DHS entities, in making award decisions. U.S. ports have been grouped into "port areas" based on regions, and then placed into one of four Groups based upon FEMA's risk evaluation model:

Group I, which are the seven highest risk port areas, includes:

- Los-Angeles-Long Beach
- San Francisco Bay
- New Orleans
- Delaware Bay
- New York-New Jersey
- Houston-Galveston, and
- Puget Sound

Figure 1. Port Security Grant Program Appropriations, FY 2002-FY 2012

Fiscal Year	Amount Allocated
FY 2002	$93,000,000
FY 2003	$244,000,000
FY 2004	$179,000,000
FY 2005	$141,000,000
FY 2006	$168,000,000
FY 2007	$202,269,793
FY 2007 Supplemental	$110,000,000
FY 2008	$388,600,000
FY 2009	$388,600,000
FY 2009 ARRA	$150,000,000
FY 2010	$288,000,000
FY 2011	$235,029,000
FY 2012	$97,500,000
Total	**$2,684,998,793.00**

Group II contains 48 port areas; Group III contains 35 port areas; and the "All Other Port Areas Group" is the catch-all for the remaining ports. FEMA uses the term "port areas" because it accounts for situations where several ports are in close geographic proximity, such as Los Angeles and Long Beach, and New York and New Jersey. See Appendix 1 for a listing of Group I, II, and III port areas.

FEMA allocates PSGP monies based upon risk. The seven Group I ports get approximately 60 percent and the 48 Group II ports get approximately 30 percent of each appropriation (or what are referred to as funding rounds). Group I and Group II port areas do not compete for PSGP grant monies; rather, within each Group individual port areas receive their pro-rata share of PSGP monies based on their individual risk ranking. Group I and Group II port areas, and in particular the seven Group I port areas, have become accustomed to an annual multi-million dollar windfall of PSGP monies. They have used these funds to purchase a Pentagon-like array of security systems, including high-resolution cameras, radar systems and even sonar sensors. In contrast, Group III and "All Other Port Areas Group" must directly compete for the remaining ten percent of PSGP monies.[8]

For FY 2012, a total of $97.5 million dollars has been appropriated to the PSGP as follows.[9]

Figure 2. Port Security Grant Program FY 2012 Appropriations

	Number of Applications Submitted	Number of Projects Submitted	Funding Received
Group I	81	125	$58,923,829
Group II	181	240	$29,250,000
Group III	28	38	$4,451,171
All Other Port Areas	63	83	$4,875,000
Total	**353**	**486**	**$97,500,000**

Notably, the PSGP's funding solicitation criteria—formally known as the "Funding Opportunity Announcement or FOA"—has focused on physical security projects. *While cybersecurity projects can certainly fit within the FOA criteria, to date, cybersecurity has never been an expressly stated criteria in a PSGP FOA solicitation.* Therefore, through a series of site visits, interviews, and case studies, this research paper attempts to identify whether any PSGP projects in the ports it examined are directly related to cybersecurity and explore how the PSGP program might be used to incentivize cybersecurity projects on a going forward basis.

Notes

[1] Transportation Research Board, "The Marine Transportation System and the Federal Role: Measuring Performance, Targeting Improvement," Special Report 279, 2004, http://www.cmts.gov/downloads/TRB_279_Report.pdf, accessed April 2013.

[2] U.S. Department of Transportation, "Ports," Maritime Administration, http://www.marad.dot.gov/ports_landing_page/ports_landing_page.htm, accessed April 2013.

[3] International Longshoremen's Association (ILA), http://ilaunion.org/, accessed April 2013.

[4] *See* 33 Code of Federal Regulations, Subchapter H, Parts 101-107. Part 104 covers vessels and Part 105 covers facilities.

[5] Mickey McCarter, "Coast Guard Proposes Long Awaited Rule for TWIC Readers," *Homeland Security Today*, March 25, 2013, http://www.hstoday.us/briefings/industry-news/single-article/coast-guard-proposes-long-awaited-rule-for-twic-readers/3ab28f831c1f42c2e43bae42dd1c8326.html.

[6] U.S. Government Accountability Office, "Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could be Strengthened," GAO-12-47, November 17, 2011, http://www.gao.gov/products/GAO-12-47.

[7] Alexander Mrazik, Federal Emergency Management Agency, Branch Chief Port Security Grant Program, interview with the author.

[8] U.S. Government Accountability Office, "Port Security Grant Program."

[9] Ibid. The FY2012 PSGP funding was a significant reduction from the FY2011 level. Congress dramatically reduced the funding level due to budget cuts as well as its perception that ports were not spending down previously allocated PSGP monies at an acceptable rate.

CHAPTER THREE
Into the Ports

The East Coaster – Maryland Port Administration (MPA) and The Port of Baltimore (POB)[1]

The situation in Baltimore aptly illustrates the high tech nature of America's ports, but also their resultant vulnerability. As container ships put their lines over to moor at MPA's container terminals in the Port of Baltimore, which MPA leases to Ports America Chesapeake, computerized cargo and terminal management systems are instantly triggered. Networked state-of-the-art gantry cranes then begin offloading containers. Software systems tell the equipment operators and stevedores where in the terminal to place the cargo and how it will travel to its next destination, i.e., via railcar or truck. Wireless networks allow equipment operators and stevedores to continuously view and update data in the logistic management database via handheld scanners and other smartphone-like devices. Notably, because the container terminal operations are run by Ports America Chesapeake, a private entity, MPA does not have detailed visibility on their networks, ICS systems, or proprietary terminal management systems.

At the other end of the terminal, eModal—the Port's comprehensive terminal management software—not only controls cargo but also access control.[2] Prior to entering the port, truckers must have previously registered with eModal on MPA's website. Once they have done so, they are provided a radio frequency identification tag (RFID). As they enter and exit with their cargo, networked systems electronically scan them in and out of the port while simultaneously taking imagery of their departure (which is recorded to networked servers). Other vendors and visitors with business in the port must preregister with mVisitor, a computerized personnel access control system designed by MPA authorities. Some 700-800 vendors that regularly do business in the port are currently registered with mVisitor. Meanwhile, MPA's staff watches over port operations with 400-500 networked security cameras, many of which are linked through MPA's wireless networks that span the port and operate on several frequencies. MPA officials are able to view and record this imagery on their computer terminals. MPA's network is supported by an in-house IT staff and takes advantage of the larger Maryland Department of Transportation (MDOT) network.

MPA has reported cyber incidents, to include attempts by hackers to access their system. However, since their network is part of MDOT, it is unclear whether these attacks were specifically directed at MPA or more broadly at MDOT. MPA has also experienced attempts to hack into its wireless network. They believe this activity is the result of crewmembers on visiting ships attempting to gain free WiFi access. The Port

IT staff has installed commercial applications that perform system monitoring and firewall functions. Other network management monitoring and support is provided by MDOT and its contractors. MPA conducts security training for its employees prior to granting them network access. MPA expects that its response to and recovery from a cyber attack would benefit from the assistance of MDOT's IT and cybersecurity contractor and views the FBI as its government partner in a cyber response.

A disruption to any of MPA's or its terminal lessees' networked systems would quickly disrupt cargo operations and slowly ripple out to impact the one-third of the U.S. population that resides within an overnight drive of POB. And yet, the cybersecurity culture is not high. While MPA officials expressed general awareness of cybersecurity threats from media reports and the security director's recent attendance at an FBI Infragard meeting, MPA did not cite cybersecurity as one of its top challenges.[3] *It had not conducted a cybersecurity vulnerability assessment nor had it developed a cybersecurity response plan.*

MPA's security focus remains on compliance with the Coast Guard's physical security inspections. It has invested more than $7 million dollars of PSGP grant monies since 2008 into physical security enhancements, including a Visitor Access Control Center, various camera systems, thermal imaging devices, and even a Mobile Sonar Instruction System. *However, MPA has never sought PSGP monies to support a cybersecurity project.*

The Gulf Coaster – Port of Houston Authority (PHA)

Port of Houston illustrates the scale of our modern ports, especially those integral to our energy security. As a large oil tanker enters the 52-mile Houston Ship Channel and transits up the 25-mile complex that is the Port of Houston—the largest petrochemical complex in the U.S. (and the second largest in the world)—a sophisticated fiber optic network of security cameras, radars, sonar sensors, and other systems operated by the PHA, the Houston Ship Channel Security District (HSCSD), and the Houston Police, not to mention the Coast Guard's Vessel Traffic Control system, keeps watch.[4] Approximately 25 percent of oil imported to America is transported by tankers up this channel for processing into gasoline by its refineries, including the nation's largest refinery with a capacity of 567,000 barrels a day.

Any disruption to traffic on the ship channel and its more than 150 port facilities would send not just a ripple, but a shockwave, through the U.S. economy. The Port of Houston is quite literally the fuel line (and the chemical supply line) to a large swatch of the nation. Yet PHA's phalanx of federal, state, and local security officials remain focused on physical security threats and indeed authorities lack port-wide cybersecurity knowledge for structural reasons. Most of the 150 port facilities where oil and gas tankers and chemical ships will call are in private hands. Networked systems govern

their operations, from the logistics of deliveries to the refining process of their cargos. What, if any, cybersecurity measures these port facilities have in place, however, is mostly known only to the entities that own and operate these terminals.

PHA owns, oversees and operates Port of Houston's eight public terminals. PHA is a limited operating port, leasing some terminals and operating others itself. A vessel calling at one of PHA's terminals would cause the NAVIS SPARCs logistics management system to spring into action.[5] NAVIS is designed to manage all facets of terminal and cargo operations; it employs, among other things, optical character recognition to scan cargo and manage its movement.[6] When cargo exits the port by truck or rail, not only does NAVIS electronically log the cargo out and thus simultaneously functioning as part of PHA's security access control system, it also generates billing invoices for PHA. PHA's gantry cranes, fuel farms, and even its HVAC systems are networked.

PHA monitors its terminal operations from a state of the art coordination center with a 24/7 watch. However, like its cargo operations, much of PHA's physical security relies upon networked systems. PHA's gate access control systems, including cameras and electronic TWIC readers, are also networked. So is the dispatching of its more than 50 sworn police officers and almost 60 firefighters. PHA has used the substantial PSGP monies it receives as a Group I port area to build out these networked security systems. However, it has also sought and been approved to use PSGP monies for projects that have a dubious impact on enhancing security. For instance, almost $15 million in PSGP monies was used to fund the construction of three new fireboats for PHA. *PHA has never used its substantial PSGP grant monies for a cybersecurity project.*

This is not to say that there is no awareness of cyber threats. To support PHA's security and terminal operations, PHA's in-house IT staff uses commercial firewalls and other software systems that control access and monitor vulnerabilities. PHA controls physical access to its servers, networks, and ICS systems. The staff has mapped their network, including non-computerized networked systems. It has also hired outside experts to conduct "penetration testing" on its network. The results of these tests were presented to management to justify funding for cybersecurity initiatives such as the purchase of next generation firewalls, limiting the number of system entry points and patching holes in the system. *However, many basic cyber hygiene steps are not being taken. New employees do not receive cybersecurity training before being granted network access, and private stevedore company employees hired by PHA to conduct cargo operations use their own laptops to connect to PHA's cargo management system.*

Figure 3. Port of Houston Port Security Grant Program Projects, FY 2007-FY 2012		
Award FY	**Project Title/Description**	**Award Amount** (does not include port's cost-share where applicable)
FY2007	Fiber Optic Cable Installation Turning Basis	$3,749,207
	TWIC Card Implementation-Installation BCT/BPT	$1,582,861
FY2008	Fireboat Tellepsen	$4,990,000
	Fiber Network BCT, Care, BPT - Design	$983,173
	Fiber Network BCT, Care, BPT - Installation	$6,410,125
	Port Coordination Center Expansion – Design (adds office space including training room that can also be used for disaster response operations and barracks)	$169,500
	PCC Expansion – Construction	$1,412,500
	Blue Force Tracking – Computers (installs computers in port police vehicles and provides for centralized dispatch tracking of vehicles and historical data)	$597,500
	PCC Upgrades -- Reconfigure	$137,566
FY2009	Fire Department Computer Dispatch System	$317,564
	Night Vision Capability (22 Cameras)	$572,616
	CCTV Camera Replacement (105 Cameras)	$900,000
	Security Maintenance Program – 1 (maintenance funding for IT systems including cameras, TWIC readers, server and software upgrades)	$3,000,000
	Replace Fireboats Bracewell & Farnsworth	$9,980,000
FY2010	BCT Internal Fiber Improvements – Design	$100,000
	BCT Internal Fiber Improvements – Installation	$1,450,000
FY2011	Fiber Sam Houston to Southside – Design	$100,000
	Fiber Sam Houston to Southside - Install	$1,450,000
	Security Maintenance Program – 2	$1,000,000
FY2012	Fire Department Scuba Gear	$366,350
	Security Maintenance – 3	$1,100,000
	Total	**$40,368,962.00**

While PHA is generally aware of cybersecurity threats from media reporting and an FBI Infragard presentation at a recent Houston-Galveston AMSC meeting, PHA did not cite cybersecurity as one of its top three challenges or threats. PHA's reported cyber incidents include attempted "brute force attacks"—a common industry term for using internet applications to attempt to crack passwords and gain system access. The PHA IT staff also has concerns with managing portable flash drives and the "bring your own device" (BYOD) smart phone and tablet program because of the variety of devices they have to secure.

Notwithstanding PHA's reliance on networked systems for their terminal operations and security, the IT department has not done a cybersecurity vulnerability assessment on its systems. Nor does PHA have a cybersecurity incident response plan. If PHA were the victim of a cyber attack, it does not view any federal government agency as a partner. Rather, it would rely upon in-house IT staff to manage any response.

The scale of these kinds of vulnerabilities should not be understated. If PHA's networks went down, so would many of its advanced security systems. And, if the NAVIS system were to go down, PHA's terminal operations would cease. A cyberattack that caused a major disruption to the Port of Houston would be catastrophic, impacting 70 percent of all containerized cargo coming into the Gulf of Mexico as well as a large portion of the American energy supply.

The West Coast's Giant Twins – The Ports of Los Angeles and Long Beach

On the West Coast, the Ports of Los Angeles and Long beach illustrate the reach and importance of keeping American ports running smoothly to not only the U.S. economy but the world economy. Having just crossed the Pacific Ocean, two of the world's largest container ships, one from COSCO, the national flag carrier of the People's Republic of China, and the other from Hanjin, Korea's largest shipping company, start their inbound transit to the Port of Long Beach (PLB). They are each laden with thousands of containers filled with electronics, plastics, furniture, clothing, and other Asian imports that have become part of the modern American lifestyle. Inbound in the adjacent channel to the Port of Los Angeles is an oil tanker, arriving from Saudi Arabia, with thousands of barrels of crude aboard that will power Americans' ongoing love affair with the automobile—a romance that is especially passionate in California. Foreign imports account for almost 50 percent of California's gasoline supply, with the vast majority of tankers arriving at the deep water Ports of Los Angeles or Long Beach since most other California ports are too shallow to accommodate deep draft tankers.

The container liners' progress is tracked by high definition cameras, radars, sonars, and other sensors, and the data is relayed over fiber optic networks back to

security officials embarked in PLB's $21 million PSGP-funded Command and Control center. Simultaneously, progress is tracked by a separate and similar technological marvel of PSGP-funded military-grade systems, including several of PLA's more than 400 cameras that are networked to the new $43 million Port of Los Angeles Police Headquarters watch floor. Pilots responsible for guiding these vessels to their terminal also rely on global positioning systems and other networked devices to safely navigate the harbor.

As the vessels moor at their respective leased terminals, container terminal management software systems instruct stevedores operating the giant gantry cranes to offload the containers directly onto awaiting rail cars. More than 40 percent of these containers will travel inland by rail as part of the just-in-time inventory supplying U.S. retailers and consumers. Logistics management software undergirds all facets of the 16,000 containers that PLB handles each day.

Networked control systems will also govern the pumps that offload crude oil as well as much of the refining process that will turn it into gasoline, diesel, and jet fuel for California's thirsty transportation sector. *A cyber disruption here would impact 20 percent of the U.S. maritime transportation system. In just a matter of days store shelves throughout the country would start to run empty, and the movement of 17 million Southern Californians, along with their economy, would be idled.*

The Port of Long Beach

PLB has made substantial investments in security, with many of these investments funded by the more than $100 million in PSGP monies it has received since 2001.[7] PLB has a robust network infrastructure supported by a professional in-house IT staff.[8] It also uses private IT contractors as needed. Rather than placing their network on the backbone of the City of Long Beach's network, PLB made a heavy investment of more than $35 million over the past five years to build out its own infrastructure, including primary and backup secure fiber and wireless networks. These networks are what carry a vast array of data, including feeds from PLB's security cameras, radar system, and sonar stations, back to its command center. Moreover, PLB's network also has the capability to control access and adjust who has access to doors and other entry points throughout the facility.

While PLB's port operations and security are undergirded by networked systems, unlike broader national assessments it did not cite cybersecurity as one of its top threats or challenges. Rather, PLB stated that its largest challenge was that, in a port of its size, it lacks a good real-time understanding of port activities such as cargo operations, cruise ship embarkations, and special events. The port has some 26 federal, state, municipal, and industry stakeholders operating within it and has challenges coordinating their various activities even during routine operations. To expand

awareness, PLB has embarked upon an ambitious project called the "Virtual Port System" to develop a network that provides a common operating picture to share information and enhance joint awareness and collaboration. Virtual Port is funded by PSGP monies and modeled on an early DHS effort called Virtual Cities that was intended to create a similar common operating picture for all major U.S. cities. Virtual Port seeks to integrate vetted information that is already maintained by many of these stakeholders on their private networks: the U.S. Coast Guard Marine Exchange, with ship arrival data, crew lists, and berths; U.S. Customs and Border Protection cargo manifest data; law enforcement information bulletins from the California Highway Patrol; and data from private terminal operators. Virtual Port also has the capability to integrate security camera feeds from other agencies.

Like the other ports, PLB is aware of cyber threats. PLB reports that its cybersecurity incidents include two to three "cyber storms" per year caused by hackers using distributed denial of service attacks (DDOS) or other volume-type attack methods. PLB does not allow commercial internet traffic to run on its network, adding an additional level of security. They have invested nearly $1 million in advanced commercial applications to monitor network activity, intrusions, and firewalls. PLB has mapped its network and networked systems and all access points. PLB also maintains its servers in controlled access areas that are continuously monitored. Data on servers is also backed up and replicated at an off-site location.

Once again, however, the security side of the response is low to absent. PLB's network users receive some initial training, but this does not include cybersecurity training. When visited in January 2013, PLB had not yet conducted any type of cybersecurity vulnerability assessment. They later reported that they had funded a cybersecurity vulnerability assessment at an approximate cost of just $30,000. This audit focused on the deployment of the Virtual Port system so that configuration issues can be understood and potential cyber threats identified before Virtual Port is deployed. *Still, the second busiest port in the nation does not currently have a dedicated written cybersecurity directive or response plan, nor is cybersecurity response part of any existing risk management plans.*[9]

Port of Los Angeles

As in the other facilities, PLA is keenly aware that the port's cargo movement is incredibly IT-dependent.[10] It believes that of all its various terminal operations, container operations are most at risk to a cyber attack because of their extensive reliance upon logistics management systems. Interestingly, PLA also relies on electronic data submissions by its lessees to advise them on the throughput of cargo—the number of containers, cars, cruise ship passengers, and barrels of oil that are being moved through the port. They use these reports to generate bills for their lessees, and these submissions are cross-checked against PLA observations via pier mounted cameras as well as by

wharfingers, officials who make random visual observations of cargo operations. PLA also has oversight for its City Pilots Association, which depends upon various computer systems to safely navigate ships into and out of the port.

But again, like the other Ports, PLA did not cite cybersecurity as one of its top threats. Rather, PLA's primary concern is the volume of small vessels—many of which are recreational and small commercial fishing vessels—that share its waterways with the mega sized tankers and container liners calling on its terminals. To mitigate this threat, it has invested heavily in port security patrol craft, training, and other security technologies that have been supported by PSGP monies, including $6.9 million for FY2012.

PLA's state-of-the-art police headquarters includes a command center that integrates feeds from security cameras, radar, sonar sensors, and other systems. It also features a geographic information system (GIS) that has digitized all of its property and can integrate and display all information feeds to support operations. These systems are staffed by a professional force of more than 130 sworn California police officers that receive extensive training and, when on patrol, operate craft similar to those used by the U.S. Coast Guard. It also has 42 non-sworn officers on staff.

While PLA has invested heavily in physical security, it was the only port in this study that had used PSGP grant monies for cybersecurity projects—in FY2012 PLA received $1,650,000 for cybersecurity improvements. However, PLA is a landlord port that leases its 27 terminals, warehouses, and facilities to more than 300 private entities, and it has little visibility on the security of the networked systems that ensure the uninterrupted flow of the more than eight million containers it handles each year.[11]

PLA's in-house IT staff supports its network and networked systems. The network is backboned on the City of Los Angeles' infrastructure. The IT staff has mapped its network, and the servers are maintained in secure spaces and routinely backed up. Employees receive security training prior to being granted network access, and passwords are required to be changed at regular intervals. PLA views the FBI as its government partner for any type of major cybersecurity threats, but this is primarily a result of the Chief of Police's former employment with the Bureau rather than a formal plan for cyber assistance. PLA stated that any response to a cyber incident would be solely within the domain of the IT staff. The security officer would only be notified if the attack impacted cargo or other port operations.

The largest port in the U.S. has not conducted a cybersecurity vulnerability assessment, nor does it have a cyber incident response plan. Like many other ports in this study, physical security is the primary focus of the security forces, and though many of its security and other systems rely on networked systems, *cybersecurity is viewed as an IT function that lies outside the security portfolio.*

Figure 4. Port of Los Angeles Port Security Grant Program Projects, FY 2007-FY 2012		
Award FY	**Project Title/Description**	**Award Amount** (does not include cost-share where applicable)
FY 2007	Waterside Detection & Protection	$2,596,022
	Command and Control System	$2,731,830
	Interoperable Communication System	$1,236,675
FY 2007 supplemental	Security System Maintenance Program	$2,550,600
	Mobile Command Vehicle	$900,000
FY 2008	Surveillance Radar	$600,000
	Information Technology Security Project	$2,000,000
	Port Police Canine Kennel	$600,000
	Tactical Radio System	$4,000,000
	CAD/RMS Management System	$2,000,000
	Security Awareness Training	$375,000
	Maritime Law Enforcement Training Center Boats	$1,118,240.97
	Port Police Boats	$1,050,000
	Port Police Dive Boat	$1,935,000
FY 2009	Integrated Command & Control Fiber Optic Project	$4,000,000
FY 2009 ARRA	Port-wide Fiber Project – Phase II – Horizontal Drill	$6,000,000
FY 2012	Port Police Waterborne Patrol Vessels	$1,875,000
	Cyber Security Improvements	$1,650,000
	Security System Integration, Maintenance, and Repair	$3,000,000
	K-9 Facility Phase II	$375,000
	Total	**$40,593,367.97**

Inland on the River – Port of Vicksburg, Mississippi's Ergon Facilities

On the Mississippi, we can see the importance of America's inland Ports and their equally high tech operations, along with their vulnerabilities. A large oil tanker enters the Southwest Pass, boards its river pilot, and navigates up-bound on the mighty Mississippi to mile marker 182, Ergon's St. James terminal.[12] Networked pump control systems assist in offloading the crude to holding tanks. Ergon's refinery in Vicksburg, which refines 25,000 barrels of crude per day, signals it can accommodate more crude, and one of Ergon's Magnolia Marine Transport Company's (MMT) 16 tug boats and 64 barges is dispatched to carry the crude the remaining 150 river miles north from St. James to Vicksburg.[13] Its progress and cargo are tracked by logistics systems transmitting data via cellular air cards from laptop workstations aboard its tugs. ERI's refinery operations involve numerous supervisory control and data acquisition (SCADA) systems, programmable logic controllers, and many other networked devices that control the maze of valves, pipelines, and transmitters critical to refinery operations.[14] Several wireless networks allow these systems to be continuously monitored and remotely controlled, which is much less expensive than installing hard-wired systems in refineries. Technicians make rounds plugging in laptops at monitoring stations throughout the facility to observe the plant's operations in real-time. The refined products are stored and then shipped to ERI's customers using MMT's tugs and barges along the Mississippi—where they may be reloaded onto larger vessels for export, carried to ports along the U.S. inland waterways, or carried via rail or truck.

Ergon and ERI are aware of the threat of cyber attack, as their operations fall within both the energy and the maritime CIKR. They report that their network is constantly being probed, typically with brute force attacks. These persistent attacks cause a lot of frustration and require vigilance; however, to date, their systems have not suffered a major interruption. In contrast, MMT was not as aware of cybersecurity challenges, mainly because very few networked systems exist on its vessels other than the laptop running cargo tracking and vessel location systems. All networked systems are managed by Ergon's in-house IT staff. They also rely on the vendors of these systems, particularly with respect to SCADA, for support.

While Ergon is aware of cybersecurity threats, it did not cite cybersecurity as one of its top challenges or threats. Its biggest challenge is managing the flow of information from the many separate systems that are populating spreadsheet-based information management systems, and integrating this data from these systems into one place from these "automation islands" is a tremendous challenge. MMT reports that its biggest challenge is human interface and data integrity; that is, ensuring that its operators input the data they are supposed to when they are supposed to.

Ergon relies upon its in-house IT staff and the vendors who provide its equipment, especially SCADA systems, to ensure it is protected. While there is one person on the IT staff who is directly responsible for cybersecurity, his primary duty is keeping servers, SCADA systems, and software running. Servers are kept in secure locations, and the IT staff conducts onsite, offsite, and archival backups. Commercial antivirus software is used, and when the IT staff is not on site, it receives notifications of any anomalies on smartphones and other devices. The IT staff has mapped out its network, however it sometimes experiences challenges keeping up with the extensive SCADA systems in the refinery. For instance, vendors have installed additional networked SCADA devices without adequately notifying IT. *Ergon's approximately 250 users do not receive any cybersecurity training before receiving network access.* MMT also reports that training its users, mostly mariners, would be challenging. Captains tend to be with the company for many years while deckhands turn over much more frequently.

Ergon is working hard to stress cybersecurity risks and mitigation strategies to senior management. *To date, Ergon has not yet conducted a cybersecurity vulnerability assessment.* As part of a Group II port area, it has received some PSGP grant monies, which it used to install security cameras and add additional data storage to save imagery from the camera systems. MMT also received PSGP monies, which it used to conduct a pilot program for sea-based TWIC readers.

As in the other ports, Ergon does not currently have a written cybersecurity response plan, nor are cyber response plans contained in any existing risk mitigation plans. Of note, Ergon does not see government as a partner in any cybersecurity response. Ergon reported that it recently attended a meeting hosted by the National Security Council on cybersecurity in the energy sector and information sharing. The company is concerned that unless legislation protects information that it discloses to the government from secondary disclosures through the Freedom of Information Act or other means, sharing its information will put it at risk from both competitors and activist groups. Moreover, it believes that DHS cyber efforts should be more inclusive for the vendors that supply the equipment (it believes DHS is not including vendors in its response efforts because it is wary that the vendors will convert this access into new business). Going forward, Ergon believes that cybersecurity will only become more challenging. The cost savings provided by the increased use of wireless SCADA systems is significant and thus will only expand.

Strategic Military Outload – The Port of Beaumont

The USNS Red Cloud, a 950-foot large, medium-speed roll-on/roll-off military cargo ship that spans the length of nearly three football fields, has just crossed through the Sabine pass and is transiting northbound for the Port of Beaumont. In the Port, the Army's U.S. Surface Deployment and Distribution Command's (SDDC) 842nd Transportation Battalion is feverishly working with stevedores, Port representatives, and

its interagency partners to ready the more than 1,650 trucks, heavy tracked vehicles, and helicopters, as well as a port opening package that enables the landing of all the equipment for an infantry brigade that will be loaded aboard *Red Cloud*. This equipment may be shipped to support warfighters on the front lines in Afghanistan, or remain at the ready as part of the Army's Prepositioned Stocks.

Also working to organize this outload, though much less visible, is the Army's global logistics management system (LMS), which allows the Army an in transit visibility (ITV) on all of its equipment from the depot to the field.[15] LMS information is entered with handheld wireless scanners and via passive scanners for shipments containing RFID tags, which is all made possible by the 842nd's wireless network.[16] *A cyber disruption here would impact almost 50 percent of all military cargo bound for overseas contingency operations and impact the U.S. military's ability to respond to crisis or conflict. Infiltration of the Army's LMS network would impact not just the Port of Beaumont but the Army's worldwide logistics operations and allow adversaries to gain visibility on the movement of Army cargo at all modes of the supply chain, from truck to rail to ocean carriers.*

Figure 5. Port of Beaumont Port Security Grant Program Projects, FY 2005-FY 2012

Award FY	Project Title/Description	Award Amount (does not include cost-share where applicable)
FY 2005	Underwater Detection System	$1,443,020.81
	Inter-Op Radio Communication System	$232,694
FY 2006	ID Card Readers & Surveillance Cameras	$524,971.59
FY 2009	Security Mini-Bus	$35,242.00
FY 2010	Under-channel Fiber Optics	$135,300
	Orange County CCTV System	$236,882
	4500 Linear Feet of Security Fencing	$140,000
FY 2012	Portable Guard Booths	$22,280.19
	Hand-held Biometric Readers	$31,875
	Total	**$2,802,265.59**

Outside of the 842nd Transportation Battalion's operations, the Port of Beaumont (PBM) itself has not invested in networked security technologies at the same level as other ports. Rather, the security officer reports, "they do it the good old fashion way."

If you have business within the port, you call the operations center dock office and get yourself on the visitor list.[17] The gate guards still use logbooks, clipboards, and fax machines. Arriving truckers are asked for TWIC identification and their driver's license; they are then manually logged in and out of the facility. One reason for this is PBM's Group II status, which encompasses several ports.[18] PBM does not receive anywhere near the level of PSGP grant monies as a Group I port like Houston, only 80 miles to the west. From 2005 to present, PBM received just $2.8 million in PSGP funding; *none of these grant monies were used to fund a cybersecurity project.*

PBM also has relatively limited ICS operations. The port administration has a staff of 40. The IT manager is a single individual who manages a stand-alone system; she uses contract support on an as-needed basis. Besides desktop workstations, networked systems include approximately 70 security cameras that are monitored by a 24/7-contract security service on four displays within a watch center. This effort is mainly focused on ensuring that vessel crewmembers who do not possess a TWIC do not depart a visiting vessel without an escort. PBM maintains a wireless network in administration workspaces but not in its terminals. PBM does not use sophisticated access control systems, nor does it operate networked terminal information management systems.

Thus, it is perhaps no surprise that PBM did not report cybersecurity as one of its top threats. Its largest challenges were budget, training, and finding the time to conduct training. The security staff is also concerned with seaborne threats as the port has a large volume of small vessel traffic, both recreational and commercial, operating in close proximity to the large commercial vessels that call on it. This concern is particularly acute for vessels carrying military cargo. The port will often work with the Coast Guard and other officials to set up a naval protection security zone around these vessels. The security staff also listed fraudulent identification as a challenge and threat as the contract security guard service does not receive a lot of training in this area. They also cited the risk of encountering an improvised explosive device.

The PBM port security officer was generally aware of cybersecurity from recent media coverage, however, it has not been a topic of discussion at PBM or local AMSC meetings. Instead, TWIC cards have been the main focus because the software that operates the readers has not kept up with the card technology. PBM maintains control over its servers by situating them in secure spaces; in fact, the IT manager's office is co-located with the server bank. PBM users do not receive any type of cybersecurity awareness training before being granted system access, and PBM uses commercially available security software to maintain its network. *To date, PBM has not conducted a cybersecurity vulnerability assessment of its network.*

In sharp contrast, the Army's 842nd Transportation Battalion is acutely aware of the threat of cybersecurity on its networks and is keenly conscious that the Army's LMS

is under a persistent threat of cyber attack. Its in-house IT personnel work closely within its chain of command, which extends all the way to the U.S. Transportation Command (USTRANSCOM) in St. Louis, to ensure its networks are protected. The Battalion's local technicians are trained to spot network issues that indicate possible external disruptions, and they continuously interface with personnel in their chain of command to maintain cyber awareness. The LMS central managers employ state-of-the-art cyber protection systems as this network is critical to the Army's worldwide operations. *USTRANSCOM officials recently conducted a cyber vulnerability assessment of the 842nd's cargo management systems, and the 842nd has dedicated cyber incident instructions that set forth specific actions to take in the event of a cyber disruption or attack.* Their local personnel are trained on and exercise these instructions. In the event of a cyber attack, the 842nd views its headquarters, USTRANSCOM, as its key partner in any response and recovery. The 842nd would also presumably benefit from the Army's robust network security, which would assist it in restoring operations.

Notwithstanding its relatively strong cybersecurity culture, the 842nd did not report cyber threats as one of its top challenges. Rather, its biggest challenge is coordination of the safe outload and transport of military cargo along the Sabine-Neches waterway leading to Beaumont (the 842nd also has responsibility for military cargo operations in several other regional ports, including Port Arthur and Corpus Christi) which is about an eight hour transit to the Gulf of Mexico. Similar to PBM's comments, the 842nd is very concerned with the safety and security of vessels carrying military cargo that must navigate the busy and, in places, confined 42-mile Sabine-Neches waterway that includes both large commercial traffic, like petroleum and chemical tankers transporting hazardous cargos to shore-side facilities, and small commercial traffic such as fishing vessels.[19] The 842nd works closely with its federal partners, including the Coast Guard and the FBI, as well as state and local security partners to coordinate the safety of all military cargos.

While military outload operations in the busiest U.S. military strategic port embarkation benefit from the U.S. Army's attention on protecting its global logistics network, PBM, which is also an important port because of the non-military cargo it handles, is not at all focused on cybersecurity. Indeed, two pipeline terminals that supply 55 percent of the U.S. strategic oil reserves are located along the waterway, as are refineries that produce 60 percent of the nation's jet fuel, including the majority of U.S. military aviation fuel and 11 percent of the U.S. gasoline supply.[20] Overall, facilities on this waterway import more crude oil than any other port area in the U.S. While more study needs to be done, the apparent lack of focus on cybersecurity is concerning as the Sabine-Neches waterway is a vital part of the U.S. maritime transportation system and U.S. energy supply.

Notes

[1] An in person port visit, tour, and interview were conducted with the head of security for MPA, David Epsie, along with the head of IT, John Cumberledge, representatives from Ports America Chesapeake that lease space from MPA for container terminal operations, and a representative from Coast Guard Sector Baltimore on January 7, 2013.

[2] eModal, 2012, http://emodal.com/anondefault.aspx?ReturnUrl=%2f, accessed April 2013. The Port of Baltimore also hosts a page for trucking companies and drivers on its website detailing how to register with eModal. *See* Maryland Department of Transportation, "Port Security," Port Administration, http://www.mpa.maryland.gov/content/port-trucks.php, accessed April 2013.

[3] Infragard, http://www.infragard.net, accessed April 2013. InfraGard is an FBI outreach program that seeks to establish public-private partnerships with businesses, academic institutions and the private sector on cybersecurity; encourages information sharing on intrusion incidents and system vulnerabilities; and provides a channel for two-way communication of cyber threats.

[4] Houston Ship Channel Security District, http://www.hscsd.org/about.html, accessed April 2013.

[5] Navis, part of Cargotec Corporation, is used by facilities throughout the world to manage their cargo and its movement through terminals. *See* Navis, "About Navis," www.navis.com/about, accessed April 2013.

[6] Marcus Woodring, Port of Houston Authority Managing Director of Health, Safety, Security and Environmental Branch (HSEE), and Michael McClellan, Port of Houston Authority Information Technology Director, interviews with the author.

[7] J. Christopher Lytle and Sam Joumblat, "The Harbor Department of the City of Long Beach: Comprehensive Annual Financial Report Year ended September 30, 2012," http://www.polb.com/civica/filebank/blobdload.asp?BlobID=11045, p. 16, accessed May 2013.

[8] Dan Kane, Director of Security, Port of Long Beach, and Michael McMullen, Lead IT Project Manager, Security Division, interviews with the author.

[9] Port of Long Beach, "Facts at a Glance," http://www.polb.com/about/facts.asp, accessed April 2013.

[10] George P. Cummings, Director of Homeland Security and Policy Administration, Port of Los Angeles Port Police, interview with the author.

[11] Port of Los Angeles, "Port of Los Angeles (Harbor Department of the City of Los Angeles) Comprehensive Annual Financial Report, June 30, 2012 and 2011," Harbor Department of the City of Los Angeles, November 9, 2012, http://www.portoflosangeles.org/Publications/Financial_Statement_2012.pdf, pp. 2-3.

[12] Ergon, "Welcome," http://www.ergon.com, accessed April 2013.

[13] Magnolia Marine Transport, http://www.magnoliamarine.com, accessed April 2013.

[14] Steve Elwart, Ergon Refining, Director of Systems Engineering, and Paris Stokes, Magnolia Marine Transport, Information System Analyst, interviews with the author.

[15] Michael Arnold, Commanding Officer 842nd Transportation Battalion, interview with the author.

[16] Patricia Kelly and Catherine Robertello, "Radio Frequency Identification Tags in Modern Distribution Processes," *Army Sustainment Bulletin* 43, issue 3 (May-June, 2011), http://www.almc.army.mil/alog/issues/may-jun11/rfid_moddistrib.html.

[17] Steven Davis, Director of Security, Port of Beaumont, interview with the author.

[18] Texas Group II ports include Sabine-Neches River, Beaumont, Orange, and Port Arthur; Corpus Christi; and Freeport. *See* U.S. Department of Homeland Security, "FY 2012 Port Security Grant Program (PSGP): Funding Opportunity Announcement (FOA)," Federal Emergency Management Agency, http://www.fema.gov/pdf/government/grant/2012/fy12_psgp_foa.pdf, accessed April 2013.

[19] Port of Beaumont, http://www.portofbeaumont.com/about.htm, accessed April 2013.

[20] Sabine Neches Navigation District, "Waterway Quick Facts," http://navigationdistrict.org/uploads/resource/filename/SNND_DC_2013-1.pdf, accessed April 2013.

CHAPTER FOUR
Analysis

Figure 6. Port by Port Data – Cybersecurity Vulnerability Assessment & Response Plans					
Group Type	**Port**	**Vulnerability Assessment**	**Written Response Plan**	**PSGP Monies Received Since 2007**	**Use of PSGP for Cybersecurity Project**
Group I	Port of Houston	No	No	$40,368,962	$0
	Port of Long Beach	Yes	No	$120,000,000 (since 2001)	$800,000 (indirect)
	Port of Los Angeles	No	No	$40,593,367.97	$1,650,000
Group II	Port of Baltimore	No	No	$6,903,292	$0
	Port of Beaumont	No	No	$0	$0
	Port of Vicksburg-Ergon	No	No	$0	$0
N/A	842nd Transportation Command - Beaumont	Yes	Yes	N/A	N/A

Cybersecurity Awareness and Culture

While the majority of ports visited were generally aware of cyber threats, this general awareness was typically garnered from media reports or attendance at a singular cybersecurity presentation. This low-level awareness did not often translate into any follow-on action. *Thus, not only is cybersecurity awareness in U.S. port facilities generally low, but the cybersecurity culture in U.S. port facilities is generally lacking.* This is evidenced by the fact that most ports remain concerned with impacts to their day-to-day operations. The low level of cybersecurity culture is also likely a function of the fact that none of the facilities visited had sustained a disruptive cyber attack. But it is also a result of mismatched incentives. As the data shows, and as evidenced by the use of PSGP grant monies, both publicly and privately owned port facilities are more inclined to direct their security resources to traditional MTSA-required physical security measures. After all, this is what Coast Guard port facility inspectors are holding them accountable for. These port facilities are simply directing resources to the area where they currently receive regulatory security—cybersecurity is not at the top of their list, and in most cases it has yet to even make it onto their list.

Prevention and Preparedness

The level of cybersecurity prevention and preparedness in the port facilities studied varied greatly. All ports visited employ a broad range of networked technologies to manage both their operations and facility security. These operations are typically supported by IT staffs trained in network security. Ports that had higher levels of prevention measures in place benefited from being on the backbones of larger networked systems. Examples include MPA's Port of Baltimore and MDOT's IT network, which has contracts with L-3 STRATIS for a full suite of network services, and the Army's operations in Beaumont, which benefits from the Army's global logistics management system.[1] *However, most ports were not taking basic cyber hygiene steps, such as ensuring that system users receive cybersecurity training prior to granting them network access.* Moreover, of all port facilities studied, only the Port of Long Beach had conducted a cybersecurity vulnerability assessment (the U.S. Army had done an assessment for its 842nd Transportation Battalion but the Port of Beaumont, which it operates within, had not).

Several features of the Port of Long Beach's cybersecurity vulnerability assessment are notable. First, it was conducted after the author's visit in January 2013, so it was a very recent initiative. Second, the impetus for the PLB cyber vulnerability assessment was the deployment of the Virtual Port system which, by design, will leverage feeds from many other law enforcement networks. Thus, while commendable, it was not spawned by a need in normal port business. But most interestingly, *PLB reported that its assessment only cost $30,000.* This is an exceedingly low sum, and further study is needed to determine whether this figure is a representative cost estimate for assessments in other port facilities. And when compared to the $97 million in PSGP funds appropriated for FY2012, $30,000 is certainly a very low figure. Within the seven Group I Port Areas, which were allocated $58.5 million of the 2012 PSGP's $97 million, there are 33 ports. *Assuming that cybersecurity vulnerability assessments could be conducted at these 33 individual ports at the same cost as PLB, it would cost $990,000 – just less than $1 million to conduct assessments at all Group I port facilities.* Of course, within each of these port facilities there are a number of lessees and private terminal owners that are also regulated port facilities, and the cost would certainly vary. However, the point is that the cost of conducting cyber vulnerability assessments appears to be relatively low compared to the costs of a successful attack. Moreover, these cybersecurity vulnerability assessments could easily be funded by the PSGP.

Response and Recovery

The level of response and ability to recover, or resiliency, was relatively low in all ports studied. This is evidenced by the fact that not a single port had a dedicated cyber incident response plan (with the exception of the Army's 842nd Transportation Battalion). Moreover, cyber response plans were also not contained within broader risk

management plans. Interestingly enough, all the studied ports employed a dedicated security officer and a dedicated IT staff, but the security officers' focus generally remained on traditional physical security threats, and IT was a separate and distinct department from security. Cybersecurity threats were not part of the security officer's response portfolio. Most security officers assumed that their IT staff would notify them in some form or fashion if a cyber incident threatened port operations, though when during the response this notification would be made is unclear given the lack of any written response plans.

PSGP Grants – Challenges and Opportunities

As discussed throughout this paper, the PSGP program has bestowed billions of dollars upon port facilities and hundreds of millions upon the largest U.S. ports to reduce their vulnerability to terrorist attacks. Unfortunately, the PSGP program's threat analysis and resulting grant funding guidance has, to date, failed to consider the threat of a cyber attack in its calculus. This has resulted in major U.S. ports investing in an array of security systems like command centers, radars systems, and even sonar sensors akin to a Combat Information Center on a naval destroyer. *Ironically, many of these highly advanced security systems are networked, and without adequate cybersecurity, they could put the security of these ports at even greater risk to disruption from cyber threats.* Additionally, these systems are extremely expensive to purchase and to operate. If Congress continues to draw down the annual appropriation for the PSGP, it's questionable whether these ports will have sufficient funding to cover the operations and maintenance cost for these systems going forward.

Of note, there are also a number of other ostensibly security-related purchases made with PSGP monies that, on their face, do not seem to enhance security at all. For instance, the Port of Houston Authority purchased almost $15 million in fireboats with PSGP monies since 2007. Other ports have also used PSGP grants to update their fireboat fleets to the tune of millions of dollars. Fireboats are certainly important to safety, but less so to security.

The PSGP also has a cost-share requirement. Publically owned port facilities must provide a 25 percent cost-share; private port facilities must provide a 50 percent cost-share. In practice, this policy not only institutionalizes an inherent cost disadvantage for private terminals that want to accomplish security projects, but it also exacerbates the different risk and cost perspectives between public and private port facilities. *The private sector tends to view security as a cost – while the public sector tends to view security as an investment.* By making private facilities pay a larger cost-share for port security grant projects, this furthers the public-private risk perspective dichotomy. However, in application, the cost-share rules have been inconsistently applied. For instance, Congress has chosen to waive the cost-share requirements for certain grant funding rounds, including the supplemental monies appropriated to PSGP as part of the 2009

American Recovery and Reinvestment Act (ARRA) and more recently for the 2010 and 2011 PSGP appropriations. Predictably, this has caused PSGP grant applicants to attempt to reprogram earlier proposals into subsequent non-cost-share funding rounds.

Figure 7. Port Security Grant Program Cybersecurity Projects, FY 2005-FY 2012 (As provided by FEMA PSGP Program)

Award FY	Project Title/Description	Port Area	Award Amount (does not include cost-share where applicable)
FY2008	Secure Information Sharing System for Gloucester Marine Terminals	Group I Delaware Bay	$353,730
	POLA Information Technology Security Project	Group I LA-LB	$2,000,000
FY2009	Seattle IT Cyber terrorism prevention (PRISEM)	Group I Puget Sound	$896,485
	Port of Tacoma Security System Storage Area Network Ops & Maintenance	Group I Puget Sound	$247,346
FY2010	Hueneme IT System Security	Group II Hueneme IT System Security	$80,283
FY2012	POLA IT Cybersecurity Network	Group I LA-LB	$1,650,000
	Hampton Roads Cyber Systems Security	Group II Hampton Roads	$349,500
	Port of Houston Modernize and Secure the Port Security Network	Group I Houston-Galveston	$93,750
	Ponce Regional Integrated Security Knowledge System/Prevention Response	Group III Ponce, Puerto Rico	$32,508
		Total	**$5,703,602.00**

Since the PSGP program has not expressly identified cybersecurity as a part of their FOA criteria, there has been a dearth of cybersecurity proposals for PSGP monies. *For instance, there were no cybersecurity projects prior to award year 2008, there were none in award year 2011, and during the program's life there have been just nine total cybersecurity projects awarded at a total cost of less than $6 million.* Given that the PSGP has awarded $2.6 billion since its inception in 2002, the cybersecurity projects funded to date have constituted a *de minimus* amount of PSGP funding.

Given the national focus on cybersecurity, including the recent Presidential Executive order and Policy Directive, this should and must change. PSGP monies

represent a great opportunity to enhance cybersecurity within U.S. port facilities, and implementation would only take a few simple steps. For instance, FEMA's PSGP FOA could expressly identify cybersecurity as a priority. Congress could further incentivize cybersecurity projects by waiving PSGP cost-match requirements. Indeed, it appears the Secretary of DHS even has some discretion to waive the cost-match requirement for critical projects.[2] For example, when the Secretary asked that each port area produce a Port Wide Security Plan (PWSP), she allocated PSGP monies for this purpose and waived the cost-share requirement. The Secretary could take similar action by seeking to have each port facility undertake a cybersecurity vulnerability assessment, as well as prepare a cyber incident response plan, with no-cost-share PSGP monies. Moreover, as discussed above, these cybersecurity initiatives appear to be less costly than many other recent PSGP projects. Certainly, the Secretary's ability to have port facilities undertake these steps would be significantly bolstered if cybersecurity legislation provided her and DHS component agencies the authority to mandate these actions.

Conclusion

Taking steps to enhance cybersecurity in U.S. port facilities as part of the broader set of cybersecurity initiatives to protect other sectors of U.S. CIKR will greatly enhance the security and resiliency of this lesser-known but vitally important sector. This research indicates that while the awareness of current cybersecurity needs and culture in U.S. ports is relatively low, many of the steps to improve this situation are relatively simple and can be done now. The PSGP's resources present a tremendous opportunity to incentivize and fund some of these initial steps, including conducting a baseline round of cybersecurity vulnerability assessments in port facilities.

Existing structures such as the robust AMSCs should also be leveraged to provide coordinated communication of the threat, and steps that can be taken now to mitigate and minimize cyber vulnerabilities, including adding cyber incident response procedures to area maritime security plans and individual facility security plans. While Congress continues its effort to pass comprehensive cybersecurity legislation, the full suite of existing authorities should also be scrutinized to see how they might be applied in the interim or the absence of comprehensive cyber legislation. In the end, cybersecurity in port facilities should not be viewed as a regulatory intrusion into a new domain, but rather as a natural extension of the existing suite of security measures required to protect our ports, which our homeland and national security depend upon, and which U.S. economic security has relied on since the earliest days of our nation.

Notes

[1] "L-3 Awarded $42.9 Million Contract from Maryland Department of Transportation," L-3 IT Enterprise Solutions press release (Reston, VA, September 24, 2009), http://www.l-3stratis.com/images/mdot_award.pdf.

[2] *See* 46 U.S.C. § 70107 – Grants. Section (c)(2)(B) states: Higher level of support required. If the Secretary determines that a proposed project merits support and cannot be undertaken without a higher rate of Federal support then the Secretary may approve grants under this section with a matching requirement other than that specified in paragraph (1).

CHAPTER FIVE
Recommendations for Action

For the Congress:

1. Initiate a study on what cybersecurity protections should be required in port facilities and what resources the Coast Guard, as the Sector Specific Agency for maritime critical infrastructure, would require to conduct cybersecurity vulnerability assessments and other cyber inspections.

2. Develop draft legislation to grant the Coast Guard specific authority to enforce cybersecurity standards for maritime critical infrastructure, possibly as part of a larger cybersecurity bill for all sectors of critical infrastructure. The legislation should use cybersecurity standards created by NIST and maritime industry collaboration that are expressly tailored for port facilities (leveraging current efforts directed by the Presidential EO and PPD). The Coast Guard will also require authority to invest in training its inspectors in cybersecurity, or alternatively, the ability to initially contract out cybersecurity inspectors or some combination of both until it builds an inspection force with the necessary cyber expertise.

For DHS and the Port Security Grant Program Administrators:

1. Incorporate cybersecurity risk factors into current Port Security Grant Program risk modeling.

2. Expressly solicit cybersecurity projects in the Funding Opportunity Announcement (FOA) for upcoming rounds of Port Security Grant Program funding.

3. Expressly authorize the use of PSGP monies for port facility cybersecurity assessments (possibly using the Secretary's authority to waive the cost-share requirements for these assessments).

4. Expressly authorize the use of PSGP monies for port facility cyber incident response plans (possibly using the Secretary's authority to waive the cost-share requirements for these assessments).

For the Coast Guard:

1. Conduct engagement with the 43 Area Maritime Security Committees using a coordinated communication on the current threat of cybersecurity to raise awareness and provide steps stakeholders can take to mitigate this threat, including conducting cybersecurity vulnerability assessments, preparing cyber incident response plans, and other basic cyber hygiene steps.

2. Evaluate the current status of and participation in the maritime Information Sharing and Analysis Center (ISAC), and determine whether the collaboration on critical cybersecurity threats facing maritime critical infrastructure is best carried out through the existing Area Maritime Security Committees or whether a maritime ISAC is preferred—and if so ensure this body is staffed and functioning.

3. Conduct engagement with the International Maritime Organization (IMO) and other applicable international organizations to expand global maritime cybersecurity awareness, preparedness, and response standards. Initiate discussions on developing international maritime cybersecurity standards (ideally proposing the use of any port facility cybersecurity standards developed by NIST and U.S. port facility stakeholders).

4. Evaluate the existing language in the MTSA and 33 CFR 105.305 concerning "radio and telecommunication equipment, including computer systems and information networks," and determine the extent to which this MTSA authority could be used to require port facility owners to include cybersecurity in port facility security plans.

For Port Facility Owners, Operators, and Security Officers:

1. Conduct cybersecurity vulnerability assessments.

2. Draft cybersecurity response plans.

3. Design and pitch cybersecurity PSGP grant proposals.

APPENDIX I

Port Groups

Group I Port Areas	FY 2012 Allocation $58,500,000
1. Los Angeles-Long Beach	Los Angeles Long Beach
2. San Francisco Bay	Carquinez Strait Martinez Oakland Richmond San Francisco Stockton
3. New Orleans	Baton Rouge Gramercy New Orleans Plaquemines, Port of South Louisiana, Port of St. Rose
4. Delaware Bay	Camden-Gloucester, NJ Chester, PA Marcus Hook, PA New Castle, DE Paulsboro, NJ Philadelphia, PA Trenton, NJ Wilmington, DE
5. New York, NY and NJ	New York, NY New Jersey
6. Houston-Galveston	Galveston Houston Texas City
7. Puget Sound	Anacortes Bellingham Everett Olympia Port Angeles Seattle Tacoma

Group II Port Areas	FY 2012 Allocation $29,250,000
Alabama	Mobile
Alaska	Anchorage
California	El Segundo San Diego Port Hueneme
Connecticut	Long Island Sound Bridgeport New Haven New London
Florida	Jacksonville Port Everglades Miami Tampa Bay Port Canaveral West Palm Beach
Georgia	Savannah
Guam	Apra Harbor
Hawaii	Honolulu Barbers Point, Oahu Honolulu, Oahu
Indiana/Illinois	Southern Tip Lake Michigan Burns Waterway Harbor IN Chicago, IL Gary, IN Indiana Harbor, IN
Kentucky	Louisville
Louisiana	Lake Charles Morgan City
Massachusetts	Boston
Massachusetts / Rhode Island	Narragansett /Mt. Hope Bays Fall River, MA Newport, RI Providence, RI
Maryland	Baltimore
Maine	Portland
Michigan	Detroit
Minnesota	Minneapolis-St. Paul
Minnesota/Wisconsin	Duluth-Superior, MN / WI

Missouri	Kansas City
Missouri / Illinois	St. Louis, MO and IL
Mississippi	Pascagoula Vicksburg
New Hampshire	Portsmouth
North Carolina	Wilmington Morehead City
New York	Buffalo
Ohio	Cincinnati Toledo
Pennsylvania	Pittsburgh
Puerto Rico	San Juan
South Carolina	Charleston
Tennessee	Memphis Nashville
Texas	Sabine Neches River Beaumont Orange Port Arthur Corpus Christi Freeport
Virginia	Hampton Roads Newport News Norfolk Harbor
Washington / Oregon / Idaho	Colombia-Snake River System
West Virginia	Huntington – TriState
Wisconsin	Green Bay

Group III Port Areas	FY 2012 Allocation $4,875,000
Alaska	Valdez
Alabama	Guntersville
Arkansas	Helena
California	Sacramento
Florida	Ft. Pierce Panama City Pensacola
Georgia	Brunswick
Illinois	Peoria
Indiana	Mount Vernon
Louisiana	Port Fourchon / The LOOP
Michigan	Port Huron Sault Ste Marie Marine City Muskegon Monroe
Minnesota	Two Harbors
Mississippi	Gulfport Greenville
New York	Albany
Ohio	Cleveland Lorain
Oklahoma	Tulsa, Port of Catoosa
Oregon	Coos Bay
Pennsylvania	Erie
Puerto Rico	Guayanilla Humacao Jobos Ponce
Tennessee	Chattanooga
Texas	Port Lavaca – Point Comfort Victoria Brownsville
Virginia	Richmond
Wisconsin	Milwaukee
All Other Port Areas Group **Eligible entities not located within one of the port areas identified above but operating under an Area Maritime Security Plan are eligible to compete for funding.**	**FY2012 Allocation** **$4,875,000**

BIBLIOGRAPHY

American Association of Port Authorities. "Seaports and the U.S. Economy." http://aapa.files.cms-plus.com/PDFs/Awareness/US%20Economy%20Fact%20Sheet%2012-4-12.pdf, accessed April 2013.

Arnold, Michael. Commanding Officer 842nd Transportation Battalion. Interview with the author.

Clarke, Richard. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collins Publishers, 2010.

Conway, K.C. "North American Port Analysis: Preparing for the First Post-Panamax Decade." Colliers International white paper, August 2012. http://www.colliers.com/en-us/~/media/files/marketresearch/unitedstates/colliers_portreport_2012q2_final.ashx.

"Critical Infrastructure Security and Resilience." Presidential Policy Directive/PPD-21. February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Cumberledge, John. Head of Information Technology, Maryland Port Administration. Interview with the author. Baltimore, MD, January 7, 2013.

Cummings, George P. Director of Homeland Security and Policy Administration, Port of Los Angeles Port Police. Interview with the author.

Davis, Steven. Director of Security, Port of Beaumont. Interview with the author.

Elwart, Steve. Ergon Refining, Director of Systems Engineering. Interview with the author.

eModal. 2012. http://emodal.com/anondefault.aspx?ReturnUrl=%2f, accessed April 2013.

Epsie, David. Head of Security, Maryland Port Administration. Interview with the author. Baltimore, MD, January 7, 2013.

European Network and Information Security Agency. "Analysis of Cyber Security Aspects in the Maritime Sector." November 2011. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts.

Ergon. "Welcome." http://www.ergon.com, accessed April 2013.

Gordon, Peter, James E. Moore II, and Harry W. Richardson, et al. "The Economic Impact of a Terrorist Attack on the Twin Ports of Los Angeles-Long Beach." Center for Risk and Economic Analysis of Terrorism Events, University of Southern California. May 1, 2005. http://research.create.usc.edu/nonpublished_reports/23/.

Homeport. "Cybersecurity." U.S. Department of Homeland Security. https://homeport.uscg.mil/mycg/portal/ep/channelView.do?channelId=-54883&channelPage=%2Fep%2Fchannel%2Fdefault.jsp&pageTypeId=13489&BV_SessionID=@@

@@1184155535.1369077996@@@@&BV_EngineID=cccdadfjllmlgfdcfngcfkmdfhfdfgm.0, accessed May 2013.

Houston Ship Channel Security District. http://www.hscsd.org/about.html, accessed April 2013.

Infragard. http://www.infragard.net, accessed April 2013.

International Longshoremen's Association (ILA). http://ilaunion.org/, accessed April 2013.

International Ship and Port Facility Code and SOLAS Amendments 2002. International Maritime Organization, 2003.

Kane, Dan. Director of Security, Port of Long Beach. Interview with the author.

Kelly, Patricia, and Catherine Robertello. "Radio Frequency Identification Tags in Modern Distribution Processes." *Army Sustainment Bulletin* 43, issue 3. May-June, 2011. http://www.almc.army.mil/alog/issues/may-jun11/rfid_moddistrib.html.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Center for Technology and National Security Policy. Dulles, VA: National Defense University and Potomac Books, Inc., 2009.

"L-3 Awarded $42.9 Million Contract from Maryland Department of Transportation." L-3 IT Enterprise Solutions press release. Reston, VA, September 24, 2009. http://www.l-3stratis.com/images/mdot_award.pdf.

Lytle, J. Christopher and Sam Joumblat. "The Harbor Department of the City of Long Beach: Comprehensive Annual Financial Report Year ended September 30, 2012." http://www.polb.com/civica/filebank/blobdload.asp?BlobID=11045, p. 16, accessed May 2013.

Magnolia Marine Transport. http://www.magnoliamarine.com, accessed April 2013.

Maryland Department of Transportation. "Port Security." Port Administration. http://www.mpa.maryland.gov/content/port-trucks.php, accessed April 2013.

McCarter, Mickey. "Coast Guard Proposes Long Awaited Rule for TWIC Readers." *Homeland Security Today*, March 25, 2013. http://www.hstoday.us/briefings/industry-news/single-article/coast-guard-proposes-long-awaited-rule-for-twic-readers/3ab28f831c1f42c2e43bae42dd1c8326.html.

McCarthy, Charles J. "Computer Worms Pose Threat to Port Cyberphysical Systems," *American Association of Port Authorities Seaports Magazine*, Winter 2011-2012. http://digital.sea-portsinfo.com/issue/54053.

McClellan, Michael. Port of Houston Authority Information Technology Director. Interview with the author.

McMullen, Michael. Lead IT Project Manager, Security Division, Port of Long Beach. Interview with the author.

Mrazik, Alexander. Federal Emergency Management Agency, Branch Chief Port Security Grant Program. Interview with the author.

Muccin, Emil A. "Maritime Cyber Security: Survival at Sea." *Maritime Reporter and Engineering News*, July 18, 2012. http://www.marinelink.com/news/maritime-security346340.aspx.

Nakashima, Ellen. "U.S. said to be target of massive cyber-espionage campaign." *The Washington Post*, February 11, 2013, pp. A-1, 11. http://articles.washingtonpost.com/2013-02-10/world/37026024_1_cyber-espionage-national-counterintelligence-executive-trade-secrets.

National Institute for Standards and Technology Information Technology Laboratory. "Cybersecurity Framework." http://www.nist.gov/itl/cyberframework.cfm, accessed May 2013.

Navis. "About Navis." www.navis.com/about, accessed April 2013.

Obama, Barack. "Improving Critical Infrastructure Cybersecurity." Executive Order 13636. February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Obama, Barack. "2013 State of the Union Address." Speech given at U.S. Capitol, Washington, DC, February 4, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address.

Pate, Anthony, Bruce Taylor, and Bruce Kubu. *Protecting America's Ports: Promising Practices*. Report to the U.S. Department of Justice, January 2008. https://www.ncjrs.gov/pdffiles1/nij/grants/221075.pdf.

Port of Beaumont. http://www.portofbeaumont.com/, accessed April 2013.

Port of Long Beach. "Facts at a Glance." http://www.polb.com/about/facts.asp, accessed April 2013.

Port of Los Angeles. "Port of Los Angeles (Harbor Department of the City of Los Angeles) Comprehensive Annual Financial Report, June 30, 2012 and 2011." Harbor Department of the City of Los Angeles, November 9, 2012. http://www.portoflosangeles.org/Publications/Financial_Statement_2012.pdf, pp. 2-3.

"Research and Markets: Global B2C E-Commerce Trends Report 2013." *The Wall Street Journal*, April 30, 2013. http://online.wsj.com/article/PR-CO-20130430-911280.html.

Ritter, Luke, J. Michael Barrett, and Rosalyn Wilson. *Securing Global Transportation Networks*. New York: McGraw Hill Books, 2007.

Sabine Neches Navigation District. "Waterway Quick Facts." http://navigationdistrict.org/uploads/resource/filename/SNND_DC_2013-1.pdf, accessed April 2013.

Stokes, Paris. Magnolia Marine Transport, Information System Analyst. Interview with the author.

Testimony of Department of Homeland Security Secretary Janet Napolitano, Jointly before Senate Committee on Homeland Security and Governmental Affairs and Senate Committee on Commerce, Science, and Transportation hearing. *The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting our National and Economic Security*. March 7, 2013. http://www.hsgac.senate.gov/hearings/the-cybersecurity-partnership-between-the-private-sector-and-our-government-protecting-our-national-and-economic-security.

Testimony of Under Secretary of Commerce for Standards and Technology United States Department of Congress Patrick D. Gallagher, Ph.D., Jointly before Senate Committee on Homeland Security and Governmental Affairs and Senate Committee on Commerce, Science, and Transportation hearing. *The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting our National and Economic Security*. March 13, 2013. http://www.hsgac.senate.gov/hearings/the-cybersecurity-partnership-between-the-private-sector-and-our-government-protecting-our-national-and-economic-security.

The White House. "Critical Infrastructure Security and Resilience." Presidential Policy Directive/PPD-21, February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

The White House. "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets." February 2003. http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

The White House. "The National Strategy to Secure Cyberspace." February 2003. http://www.dhs.gov/national-strategy-secure-cyberspace.

Transportation Research Board. "The Marine Transportation System and the Federal Role: Measuring Performance, Targeting Improvement." Special Report 279, 2004. http://www.cmts.gov/downloads/TRB_279_Report.pdf, accessed April 2013.

U.S. Department of Homeland Security. "FY 2012 Port Security Grant Program (PSGP): Funding Opportunity Announcement (FOA)." Federal Emergency Management Agency. http://www.fema.gov/pdf/government/grant/2012/fy12_psgp_foa.pdf, accessed April 2013.

U.S. Department of Homeland Security. "National Infrastructure Protection Plan." 2009. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

U.S. Department of Homeland Security. "Transportation Systems Sector Specific Plan: An Annex to the National Infrastructure Protection Plan." 2010. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf.

U.S Department of Homeland Security. "Written testimony of U.S. Coast Guard Assistant Commandant for Prevention Policy Rear Admiral Joseph Servidio for a House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation hearing titled "Tenth Anniversary of the Maritime Transportation Security Act: Are We Safer?," September 11, 2012. http://www.dhs.gov/news/2012/09/11/written-testimony-us-coast-guard-house-transportation-and-infrastructure.

U.S. Department of Transportation. "National Port Readiness Network (NPRN)." Maritime Administration. http://www.marad.dot.gov/ports_landing_page/nprn_home/nprn_home.htm, accessed April 2013.

U.S. Department of Transportation. "Ports." Maritime Administration. http://www.marad.dot.gov/ports_landing_page/ports_landing_page.htm, accessed April 2013, accessed May 2013.

U.S. Department of Transportation. "U.S. Water Transportation Statistical Snapshot." Maritime Administration, February 2011. http://www.marad.dot.gov/library_landing_page/data_and_statistics/Data_and_Statistics.htm .

U.S. Government Accountability Office, "Cybersecurity: National Strategy, Roles, and Responsibilities Need to be Better Defined and More Efficiently Implemented." GAO-13-187, February 2013. http://www.gao.gov/assets/660/652170.pdf.

U.S. Government Accountability Office. "Maritime Security: Coast Guard Efforts to Address Port Recovery and Salvage Response." April 12, 2012, GAO-12-494. http://www.gao.gov/products/GAO-12-494R.

U.S. Government Accountability Office. "Port Security Grant Program, Risk Model, Grant Management, and Effectiveness Measures Could be Strengthened." November 2011, GAO-12-47. http://www.gao.gov/assets/590/587142.pdf.

White, Ronald. "Port Labor Talks Shift into High Gear, but Strike Continues," *Los Angeles Time*s, December 1, 2012. http://articles.latimes.com/2012/dec/01/business/la-fi-mo-ports-strike-continues-20121201.

Woodring, Marcus. Port of Houston Authority Managing Director of Health, Safety, Security and Environmental Branch (HSEE). Interview with the author.

Zernike, Kate. "Gasoline Runs Short, Adding Woes to Storm Recovery." *The New York Times*, November 1, 2012. http://www.nytimes.com/2012/11/02/nyregion/gasoline-shortages-disrupting-recovery-from-hurricane.html?pagewanted=all&_r=0.

About the Author

Commander Joe Kramek is a Judge Advocate who has provided mission support to the full spectrum of Coast Guard operations, as well as regulatory, administrative, and legislative matters. While detailed to the Department of Justice as an Admiralty Trial Attorney, he represented the United States in a broad range of maritime cases and claims. Commander Kramek also spent four years at sea conducting counterdrug law enforcement, illegal migrant interdiction, fisheries enforcement, humanitarian and search and rescue operations.

Commander Kramek holds a Masters of Law in Environmental Law from The George Washington University Law School, and a Juris Doctorate from the University of Miami School of Law. He is a 1993 graduate of the U.S. Coast Guard Academy. He most recently served as a Special Assistant to the Commandant of the U.S. Coast Guard.