Department of State

Diplomacy Laboratory

Project 20
"Private Sector Port Security Practices: Responsibilities and Best Practices"

Office of Criminal Justice Assistance and Partnership, Bureau of International Narcotics and Law Enforcement (INL/CAP)

Executive Summary

Situational Overview: Ports are complex multi-actor institutions with multiple overlaid jurisdictions. Generally, the private sector provides the majority of services for unloading and loading of cargo, yet most port security responsibilities are legally under the public sector. This series of six case studies examines "best practices" aimed at improving the management and security of the private sector to halt criminal activity as terrorism, human trafficking, narcotics, and stolen goods. Executive summaries of the case studies follow.

"Core Ports and Private Sector Management" Core American ports fall into five models, in general combining public ownership and private management. The direction is toward further privatization and landlord ports are the most common model where terminals are leased by private companies from the public sector. America has 182 ports, and core ports are rated on tonnage, number of containers (TEUs), and dollar volume. Los Angles, New York and Long Beach are highly rated in all three categories. Houston, the Port of South Louisiana, Beaumont, TX; Savannah, GA; and Norfolk, VA round out the other core ports. Quality, time and costs represent the "iron triangle" of core port reliability. All American ports are regulated by the Federal Maritime Administration (MARAD). Best practices involve improving communication and expanding the landlord model.

"Port Security and Private Sector Engagement in Port Security" Port efficiency is dependent on an interconnected system of maritime, terminal and hinterland operations. Inland Port Intermodal (IPI) is traditionally the most common method of offloading cargo and disseminating goods. The security of U.S. ports is under the jurisdiction of the United States Coast Guard (USCG) under U.S. Code Title 46, Subtitle VII, Chapter 701, and Subchapter I. Customs and Border Protection (CBP) through the Container Security Initiative (CSI) enhances the security advance screening of cargo before it is loaded onto ships coming to the US; as does the Customs-Trade Partnership against Terrorism (C-TPAT) geared towards securing the supply chain. Transportation Security Agency (TSA) helps implement security with the Transportation Worker Identification Credentialing (TWIC) by biometrically verifying personnel accessing maritime ports. Best practice recommendations note that it is imperative there be an increase in information sharing between the private and public sector through cross-governmental multi-agency collaboration plus updated safety bulletins. P25 compliant radio systems now allow ports to communicate with local law enforcement officers.

"Private Sector Elimination of Criminal Activity and Security Gaps" Private sector ports identify criminal activity and security gaps via internal security programs and external agencies. Their risk management security system established mitigates, prevents, responds, and recovers from any perceived threat. Utilizing law enforcement data and through conducting in-house security reports, criminal operations' trends and methods are located. CBP's Customs-Trade Partnership Against Terrorism (C-TPAT), integrates the private sector concerns to into the Agency's architecture. Over 10,000 firms are certified through C-TPAT and through incentives. Cameras and motion detectors have been used in ports for several decades and now ports have shifted to the digital world. Surveillance equipment such as High performance Stabilized Observation Payloads used for day and night surveillance, UAVs, helicopters, and other means improved port security. Additionally radar sensors, sonar sensors, integrated GPS and GIS mapping systems and electronic card readers for access control under the TWIC program add to security. Best practices involve improved standardized training programs imposing a national set of security standards with government providing direct subsidies for increased security measures. Communication and information sharing will improve due to the new changes in the National Terrorism Advisory System (NTAS).

"Private Sector Engagement and Public-Private Coordination in Port Security" U.S. port security is anchored in identifying gaps. Ports offer significant risks due to the sheer daily volume of cargo and individuals. Most transport is via containers and the "Trojan Horse" is the greatest fear. The other contemporary concern is cyber security regarding maritime control systems, vessel networks, tracking technology, and logics software. The Customs-Trade Partnership Against Terrorism (C-TPAT) creates enhanced worldwide supply chain security. Security training is also critical, and the United States Maritime Administration had the U.S. Merchant Marine Academy develop it. Over 17,000 maritime security personnel have attended one or more of these courses. The Federal Emergency Management Agency (FEMA)'s annual Port Security Grant Program (PGSP) is another splendid endeavor to incentivize the private sector to enhance port security. The U.S. Department of Justice successfully launched "Operation Cooperation"—a national effort to increase collaboration between the private sector and state and local law enforcement agencies. As well, through local Area Maritime Security Committees (AMSC), enhance security communication among port stakeholders and local agencies. Recommendations for best practices are: broaden ASMC membership; clearly spell out vessel diversion plans; improve incident mitigation plans; enhance port infrastructure security and expand the radiation based Vehicle and Cargo Inspection System (VACIS).

"Best Practices Recommendations for Private Sector Port Security Standard Operating Procedures (SOPs)" Port security has many contributing factors, including: shared port responsibility; difficulty ensuring security along the entire supply chain due to lax foreign ports security; plus sheer volume. President George W. Bush signed the Maritime Transportation Security Act (MTSA) linking contingency planning and enhanced communication. Effective local security Standard Operating Procedures (SOPs) became the goal. Despite the establishment of dozens of AMSCs nationally, attracting and maintaining consistent private sector participation was difficult due to budgets and travel. Releasing sensitive intelligence information also became an issue due to security clearance requirements. But subsequent Presidential Policy Directives and Executive Orders attempted to underscore the need to create effective local SOPs. Currently

each AMSC is working at providing effective SOPs for the Captain of the Port (COTP) – the port responsible Coast Guard Officer. The private sector can utilize free government resources via the America's Waterway Watch (AWW) for reporting suspicious activity. Frameworks are in place to facilitate interoperability in SOPs from the U.S. government and the International Organization for Standardization (ISO) and the World Customs Organization (WCO). Best practices entail using these frameworks to facilitate SOP interoperability. For developing SOPs, the Port Security Grant Program offers immense assistance for private sector port companies to write their port Facility Security Plan (FSP) into their SOPs.

"**Best Practices of Selected Asian Ports"** The Philippines, Vietnam, Malaysia and Indonesia ae the Asian ports. The Philippine Port Authority manages all ports save one. Under the PPA, the International Ship and Port Facility Security (ISPS) Code establishes guidelines port security. The PPA also partners with the U.S. to prevent terrorist access to nuclear materials. Vietnam is quickly becoming a global leader in exports. Vietnam has 114 seaports with 14 larger ones key to economic development. However, overall sea port connectivity is hindered by unreliable transportation infrastructure and Vietnam has a problem with corruption. In Malaysia the narrow, 550-mile waterway straddling Indonesia, Malaysia and Singapore is a key commercial maritime route carrying a third of the world's trade and half of the world's oil supply. As such, security of the supply chain at Port Klang is of particular interest to the U.S. and CBP. Indonesia comprises over 17,000 islands with 154 active ports. The majority of ports are managed by the Indonesia Port Corporation. The USCG found vast improvement following inspections conducted after Indonesia was placed on the advisory list. Best practices overall include: implementation of the ISPS Code abroad and continued U.S. partnerships. Examples of an excellent U.S. partnership were cited as key security improvements for ports in the Philippines and Malaysia. Malaysia partners with the U.S. and CBP in the implementation of the CSI to pre-screen containers. Continued funding is needed.

Methodology:

As part of the Diplomacy Laboratory, this is submitted on behalf of the Graduate Students in my "J 531Unied States National Security and Homeland Security" class of the Indiana University School of Public and Environmental Affairs at Indiana University Purdue University Indianapolis as part of their fall 2015 course requirement. All students contributed to researching the entire manuscript and to writing it systematically and sequentially, part-time, throughout the fall term. At the conclusion, they then by group, edited and wrote the respective case studies which display their names. They are all co-authors and co-researchers and co-editors of this Project.

William A. Foley, Jr., Ph.D. Faculty Advisor and Co-author

"Core Ports and Private Sector Management"

Jason Allen
Graduate Student

Kaleigh Andrews
Master of Science in Criminal Justice and Public Safety
Expected Graduation: May 2017

Kelsey Andrews
Master of Science in Criminal Justice and Public Safety
Expected Graduation: May 2017

Brooklynn Baker
Graduate Certificate in Homeland Security and Emergency Management
Expected Graduation: May 2016

Indiana University School of Public and Environmental Affairs
Indiana University – Purdue University Indianapolis

Situation:

Since September 11th, 2001 there has been an increasing concern about weapons of mass destruction (WMD) and other dangerous components that could cause serious harm. The private sectors play a major role regarding this concern because they are often the ones manufacturing and transporting individual packages that could potentially be used as a weapon if they get into the wrong hands. In order to prevent such an incident, both the private and the public sectors are required to form a functional relationship. That relationship today around the world, not just in the U.S., is not where it should be and is often replete with suspicion and animosity between the two sectors.[1] In order to prevent a future incident, lawmakers are requesting stricter regulations including increased port security, tighter export regulations, and a variety of other preventative measures.[2] Yet these types of increased measures are often difficult to follow for the private sector. The government and lawmakers are so focused on preventing a future terrorist incident that they often do not see the harm

[1] Finlay, Brian (2009, February 18). *Minding Our Business: The Role of the Private Sector in Managing the WMD Supply Chain.* Retrieved from http://www.Stimson.org
[2] Finlay, Brian (2009, February 18). *Minding Our Business: The Role of the Private Sector in Managing the WMD Supply Chain.* Retrieved from Retrieved from http://www.Stimson.org

the cause to corporate interests.[3] In order to protect the world from potential dangers, there should be a healthy, established balance between the private and public sectors.

The United States has a multitude of maritime ports in which it conducts business in importing goods, exporting goods, and transportation- all via direct ocean border location or seaway access. With 182 ports handling millions of tons of waterborne activity annually, chiefly commodities. There is a significant amount of product tonnage being brought in and out of our country annually.[4] And there are various ways we can measure which ports are central to the maritime activity of the nation.

According to the Navigation and Civil Works Decision Support Center U.S. Army Corps of Engineers, below are the top five ports based on weight in tons both foreign and domestic moving through yearly:[5]

1. **Port of South Louisiana, LA** with 238.6 million total tons
2. **Houston, TX** with 229.2 million total tons
3. **New York, NY/NJ** with 123.3 million total tons
4. **Beaumont, TX** with 94.4 million total tons
5. **Long Beach, CA** with 84.5 million total tons

Port traffic is also measured in twenty-foot equivalent units (TEUs), which refers to the standard size container (Container port traffic TEU: 20 foot equivalent units), below are the numbers for 2014.[6]

---

[3] Finlay, Brian (2009, February 18). *Minding Our Business: The Role of the Private Sector in Managing the WMD Supply Chain.* Retrieved from Retrieved from http://www.Stimson.org

[4] Navigation and Civil Works Decision Support Center U.S. Army Corps of Engineers. (2015, July 15). *The U.S.Waterway System Transportation Facts & Information 2014*. Retrieved from http://www.navigationdatacenter.us/factcard/factcard14_v1.pdf.

[5] Navigation and Civil Works Decision Support Center U.S. Army Corps of Engineers. (2015, July 15). *The U.S.Waterway System Transportation Facts & Information 2014*. Retrieved from http://www.navigationdatacenter.us/factcard/factcard14_v1.pdf.

1. **Los Angeles, CA** with 5,892,982
2. **Long Beach, CA** with 4,933,499
3. **New York, NY** with 4,276,766
4. **Savannah, GA** 2,597,825
5. **Norfolk, VA** 1,931,510

The top 5 based upon dollar value of foreign traffic, based on 2013 figures:

1. Los Angeles, CA

When the Panama Canal opened in 1914, it paved the way for Los Angeles, California to become one of our countries' largest and busiest ports, this is determined by the size and amount of traffic flow through the area.[7] The Port of Los Angeles is "North America's leading seaport in terms by container volume and cargo value," generating $290 billion in trade during 2014.[8] This port is part of the City of Los Angles and is overseen by members of the Board of Harbor Commissioners. The port along with the Los Angeles Port Police force work in close collaboration with multiple government entities to monitor and keep safe vast miles of waterfront and land-based facilities, and employs one of the most comprehensive, 24/7 threat detection and incident management systems in the world.[9]

2. New York, NY/NJ

---

[6] The World Bank. (2015). *Data: Container port traffic (TEU: 20 foot equivalent units).* Retrieved from http://data.worldbank.org/indicator/IS.SHP.GOOD.TU/countries

[7] American Association of Port Authorities (AAPA). (2013). *Glossary of Maritime Terms. AAPA.* Retrieved from http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1077.

[8] The Port of Los Angeles. (2015). *A Profile of the Port of Los Angeles. The Port of Los Angeles*. Retrieved from https://www.portoflosangeles.org/about/profile.asp

[9] The Port of Los Angeles. (2015). *A Profile of the Port of Los Angeles. The Port of Los Angeles.* Retrieved from https://www.portoflosangeles.org/about/profile.asp.

These ports moves millions of people and transports vital cargo throughout the new York/New Jersey region annually.[10] The Port Authority of New York and New Jersey conceives, builds, operates, and maintains infrastructure critical to the New York/New Jersey region's trade and transportation network.[11]

3. Long Beach, CA

The Port of Long Beach is owned and operated by the City of Long Beach. Even though both long Beach and Los Angeles are in close proximity to one another they aren't the same. "The Port of Long Beach is a public agency managed and operated by the City of Long Beach Harbor Department, and governed by the Board of Harbor Commissioners."[12] The port also works closely with the U.S. Coast Guard, Customs and Border Protection, state and federal Homeland Security offices, the Long Beach Police Department, and the Port's own Harbor patrol to ensure safety of the ports.[13]

4. Houston, TX

The Port of Houston Authority is made up of seven volunteer Harris County residents who serve as Port Commissioners. The Port of Houston consists of a 25 mile long complex, and has been ranked 1st numerous times as the nation's leader in foreign waterborne tonnage.[14]

5. Savannah, GA

---

[10] Port Authority of New York & New Jersey. (n.d.). Retrieved from http://www.panynj.gov/
[11] Port Authority of New York & New Jersey. (n.d.). Retrieved from http://www.panynj.gov/
[12] Port of Long Beach, The Green Port (2015). Retrieved from http://www.polb.com/default.asp
[13] Port of Long Beach, The Green Port (2015). Retrieved from http://www.polb.com/default.asp
[14] Overview | The Port of Houston Authority. (2015). Retrieved from http://www.portofhouston.com/about-us/overview/

All the ports in Georgia, including Savannah, are run by the Georgia Ports Authority (GPA).[15] The ports of Georgia are a quasi-state agency with a 13 member Board of Directors who governs the activities of the GPA.[16]

These ports are our core ports. It should be noted that ports across the globe are managed by regulations from various sources of governance. Ports in the US fall under an array of jurisdictions to include federal, state, local, public port authority entities, port navigation districts, municipal port departments, all of this while still accommodating some international and foreign regulatory measures to ensure agreed upon trade practice. The US has 150 deep draft seaports and 126 public seaport agencies with jurisdiction over these ports.[17] That is nearly one regulatory/enforcement agency per port. This demonstrates the varying and differing ways ports are operated and managed and the politics that are likely involved.

Public ports work closely with the private industry both in the development and financing of marine terminals and other maritime-related facilities.[18] The alignment of public and private interests determines the structure of port management and port development policies. They are used to manage port operations more efficiently and effectively.[19] Although the private sector does not generally provide port security, they purchase and install their own equipment and are responsible for terminal operations. There are several reasons why ports choose privatization over public ports, including:

- Removal of trade barriers

---

[15] Georgia Ports Authority. (2015). *About. Georgia Ports Authority.* Retrieved from http://www.gaports.com/About.aspx

[16] Georgia Ports Authority. (2015). *About. Georgia Ports Authority.* Retrieved from http://www.gaports.com/About.aspx

[17] American Association of Port Authorities. (2013). *U.S. Public Port Facts.* Retrieved from http://www.aapa-ports.org.

[18] Martino, M. (2014, February 27). *Public Sector Agencies with Private Sector Expectations.* Retrieved from http://www.nxtbook.com/naylor/AAPQ/AAPQ0114/index.php?startid=10#/10.

[19] Rapoza, K, (2014, November 11) *Forbes Investing, The World's Busiest Ports.* Retrieved from http://www.forbes.com/sites/kenrapoza/2014/11/11/the-worlds-10-busiest-ports/.

- Harnessing the efficiency and expertise of the private sector
- Elimination of political interference
- Reduced demand on the public sector budget
- Reduced expenditure on port labor[20]

We can see varying management models when looking at how our core ports operate. Port management is broken up into five models:

Public Service ports: The port authority of public service ports performs the whole range of port related services, in addition to owning the entire infrastructure. They are commonly a branch of a government ministry and most of their employees are civil servants. Some ancillary services can be left to private companies. Because of the inefficiencies they are related with, the number of public service ports has declined.[21]

Tool ports: Similar in every aspect to a public service port, the tool port differs only by the private handling of its cargo operations, albeit the terminal equipment is still owned by the port authority. In several cases, a tool port is a transitional form between a public service port and a landlord port.[22]

Landlord ports: Represents the most common management model where infrastructures, particularly terminals, are leased to private operating companies with the port authority retaining ownership of the land. The most common form of lease is a concession agreement where a private company is granted a long term lease in exchange of a rent that is commonly a function of the size of the facility as well as the investment required to build, renovate or expand the terminal. The private

[20] World Bank Port Reform Toolkit. (n.d). *Alternative Port Management Structures and Ownership Models.* Retrieved from http://siteresources.worldbank.org/INTPRAL/Resources/338897-1117197012403/mod3.pdf.
[21] Rodrigue, D. J.-P. (1998). *Public and Private Roles in Port Management. (D. o. Geography, Producer, & Hofstra University).* Retrieved from https://people.hofstra.edu/geotrans/eng/ch4en/conc4en/tbl_public_privte_roles_ports.html.
[22] Rodrigue, D. J.-P. (1998). *Public and Private Roles in Port Management. (D. o. Geography, Producer, & Hofstra University).* Retrieved from https://people.hofstra.edu/geotrans/eng/ch4en/conc4en/tbl_public_privte_roles_ports.html.

operator is also responsible to provide terminal equipment so that operating standards are maintained.[23]

Corporatized ports: Concerns ports that have almost entirely been privatized, with the exception that ownership remains public and often assumed as a majority shareholder. The port authority essentially behaves as a private enterprise. This management model is unique since it is the only one where ownership and control are separated, which lessens "public good" pressures landlord port authority are facing and "shareholder value" pressures private ports are facing.[24]

Private Service ports. The outcome of a complete privatization of the port facility with a mandate is that the facilities retain their maritime role. The port authority is entirely privatized with almost all the port functions under private control with the public sector retaining a standard regulatory oversight. Still, public entities can be shareholders and thus gear the port towards strategies that are deemed to be of public interest.[25]

The management of these ports relies on what one executive of the American Association of Port Authorities calls the “Iron Triangle,” which consists of “quality, time and cost.” The goal of running such a port, much like running any other company, is to obtain the best quality of service and product, in the quickest time, at the lowest cost. Even though maritime ports are technically within the public sector, there has been a steady shift in the industry toward the privatization of aspects of port management in order to best maximize profit within this Iron Triangle.

The ports in the United States are governed a federal agency the Maritime Administration (MARAD) and is responsible for assisting all U.S.-flagged ship carrying domestic and foreign goods.

---

[23] Rodrigue, D. J.-P. (1998). *Public and Private Roles in Port Management. (D. o. Geography, Producer, & Hofstra University).* Retrieved from https://people.hofstra.edu/geotrans/eng/ch4en/conc4en/tbl_public_privte_roles_ports.html.

[24] Rodrigue, D. J.-P. (1998). *Public and Private Roles in Port Management. (D. o. Geography, Producer, & Hofstra University).* Retrieved from https://people.hofstra.edu/geotrans/eng/ch4en/conc4en/tbl_public_privte_roles_ports.html.

[25] Rodrigue, D. J.-P. (1998). *Public and Private Roles in Port Management. (D. o. Geography, Producer, & Hofstra University).* Retrieved from https://people.hofstra.edu/geotrans/eng/ch4en/conc4en/tbl_public_privte_roles_ports.html.

The MARAD ensures all ships bring in goods are US-flag ships under the Jones Act (MARAD 2015).

> **"The Jones Act**, 46 U.S.C. 55102 (19 C.F.R. 4.80b), is one of several coastwise laws enforced by CBP which prohibits the transportation of cargo between points in the U.S., either directly or via a foreign port, or for any part of the transportation, in any vessel other than a vessel that has a coastwise endorsement, i.e. a vessel that is built in and owned by persons who are citizens of the United States."[26]

Although the MARAD is the federal agency over the U.S. ports each of the ports has its own agency that manages it. The port of Los Angeles is managed by Los Angeles Harbor commission; a five-member board makes up the administrative body of the port, appointed by the Mayor of Los Angeles.[27] The Port of Los Angeles prides itself on its world-class security operations along with homeland security operations and the nation's largest dedicated port police force.

The Port of Long Beach operations are managed by the Long Beach Harbor Commission, which is made up of over 400 employees and has 17 divisions.[28] The port is governed by the Long Beach Board of Harbor Commissioners, which are appointed by the mayor of Long Beach and confirmed by the city council. Further, the board then appoints the Port Executive Director. The Port lands are owned by the City of Long Beach in a trust for the people of the State of California and are not available to be sold to any private enterprise.

The New York & New Jersey port is controlled by the Port Authority that is governed by a six-member commission appointed by the governor of each state.[29] The Georgia Port Authority

---

[26] U.S Customs and Border Protection (2015). *What is the Jones Act?* Retrieved from https://help.cbp.gov/app/answers/detail/a_id/23/~/the-jones-act.
[27] LA, The Port of Los Angeles, America's Port (2015) Retrieved from https://www.portoflosangeles.org/idx_commission.asp
[28] Port of Long Beach. (2015). *FAQs. Port of Long Beach*. Retrieved from http://www.polb.com/about/faqs.asp
[29] Port Authority of New York & New Jersey (2015) Retrieved from http://www.panynj.gov/corporate-information/governance.html

(GPA) is the managing body for the Port of Savannah. The GPA is run by a 13 member board appointed by the Governor and each member serves a four term, staggered.[30] The Norfolk Virginia Port is also known has the Norfolk International Terminal (NIT). It has a port authority operation that is overseen by Virginia International Terminals (VIT), which is owned by the Virginia Port Authority (VPA).[31] VIT is a limited liability company consisting of single member private organization and receives no funding from the VPA.[32]

Each port management model has its strengths and weaknesses, though many large and successful ports fall under the Public Service, Tool, or Landlord Port models. In the US, our core ports are primarily landlord ports in which there is a happy medium between public ownership, oversight, private leasing, and operation. For example, the Port of Houston, Port of Long Beach, and Port of South Louisiana all have commissions that oversee the respective harbor/port authorities. The municipality that has jurisdiction over the port establishes these commissions with the mayor appointing commissioners that commonly seat them. These commissioners are then agreed upon and confirmed by a city council or board and are restricted to term limits. The commission's job is to ensure smooth operation of the port, to include: administration, nautical management, infrastructure, security, contractor oversight for ancillary services, and regulations of privatized functions such as cargo handling and superstructure (warehouses, sheds, rigs, etc.). The privatization is largely corporations leasing out the port authorities infrastructure to conduct business.[33] This medium allows for the public sector to get money from leasing the space, creates jobs for the community (private and public), all while allowing private corporations a convenient place to conduct business.

Recommended Improvements for Best Practices:

[30] Georgia Port Authority (2015) Retrieved from http://www.gaports.com/About/GPABoardMembers.aspx
[31] The Port of Virginia. (2015). *Norfolk International Terminal.* Retrieved from http://www.portofvirginia.com/facilities/norfolk-international-terminals-nit/.
[32] The Port Of Virginia (2015) *Norfolk International Terminal.* Retrieved from http://www.portofvirginia.com/stewardship/economic-development/fast-facts/.
[33] The Geography of Transport Systems. (2015). *Public and Private Roles in Port Management.* Retrieved from https://people.hofstra.edu/geotrans/eng/ch4en/conc4en/tbl_public_privte_roles_ports.html.

With any situation there is always something that can be improved upon. Each of the many U.S. ports has its own distinctions. The way the ports are operated and maintained varies, but as mentioned earlier the majority uses a landlord model. This type of model is generally more efficient because a commissioner is appointed to oversee the port and its operations. This type of role shouldn't be considered a political one, but rather an expert. In order to maintain efficiency and effectiveness within each port there needs to be someone with knowledge about that port and operations, they cannot just be a figure head. Further, there needs to be communication from top to bottom, and also with local/federal agencies. Communication both inside and outside the port is extremely important to the port operations, and the safety of the community it serves.

"Port Security and Private Sector Engagement in Port Security"

Austin Robbins
Graduate Certificate in Homeland Security & Emergency Management
Expected Graduation: May 2017

Joseph DesJarlais
Graduate Certificate in Homeland Security & Emergency Management
Expected Graduation: December 2015

Marvin Cummings
Graduate Certificate in Homeland Security & Emergency Management
Expected Graduation: May 2017

Travis DeVore
Graduate Certificate in Homeland Security & Emergency Management
Expected Graduation: May 2017

Indiana University School of Public and Environmental Affairs
Indiana University – Purdue University Indianapolis

Situation:

Maritime ports are unceasingly engaged as a medium in world trade. They are one of the prime avenues in which commodities are imported and exported to reach their desired consumer. As previously identified, the majority of ports that are successful have an even split between public and private sector involvement.

The public sector generally owns and maintains the port's land itself, as well as the primary infrastructure. Infrastructure being terminals, docks, harbors, wharfs, anchoring points, and so on- this is then leased out to corporations. The public sector also provides policy, regulation, and enforcement/security functions for the port. The private sector is responsible for superstructure development, which is any extension of the infrastructure, such as warehouses and hoists/lifts. The private sector is also generally responsible for cargo handling. Present in the most common model of port, the landlord model, the public and private sector share roles in pilotage, which is the directing of ship movement into port; towage, which is the movement of large vessels or

disabled vessels; mooring, the anchoring or docking of a boat; and dredging, the cleaning and maintenance of the port's water itself. [1]

Ports are under increasing pressure to reduce costs associated with receiving and handing cargo. Port efficiency is dependent on an interconnected system of maritime, terminal and hinterland operations. These dimensions are interconnected "since inefficiencies in one dimension are likely to impact the others".[2] Maritime operations are a critical measure in the efficiency of port operations and a factor in the overall cost of shipping. Thus the ship wait times, port capacity and consequent vessel turnaround time is a crucial measure of port efficiency and competitiveness.[3] Terminal operations are limited by critical bottlenecks such as crane performance and offloading capacity. Equally critical are hinterland operations and the speed at which cargo can be sorted and distributed. This relies on efficient trans-loading and sorting procedures, transportation infrastructure and geographic advantage. [4]

Inland Port Intermodal (IPI) is traditionally the most common method of offloading cargo and disseminating goods from port to destination. Under IPI, ocean carriers coordinate the movement of cargo from water to land, keeping the container contents intact from point of origin to distribution center. "Ocean carriers, terminal operators and railroads have developed the infrastructure and processes required to move 20-, 40- and 45-foot containers — already filled with freight and sitting on their ships — directly onto the rail lines that ran right into the harbor or to a point nearby".[5] From there,

---

[1] American Association of Port Authorities. (2013). *Glossary of Maritime Terms*. Retrieved September 29, 2015, from AAPA: http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1077

[2] Rodrigue, J.-P. (2015). *The Port Performance Continuum.* Retrieved from Hofstra University: https://people.hofstra.edu/geotrans/eng/ch4en/conc4en/port_performance_continuum.html

[3] Tongzon, J., & Heng, W. (2005). Port privatization, efficiency and competitiveness: Some empirical evidence from container ports (terminals). *Transportation Research Part A: Policy and Practice*, 405-424.

[4] Rahimi, M., Asef-Vaziri, A., & Harrison, R. (2008). *Integrating Inland Ports into the Intermodal Goods Movement System for Ports of Los Angeles and Long Beach.* Metrans.

[5] Schneider. (2015, February). *White Paper: Transloading Takes Over*. Retrieved from Schneider: http://www.schneider.com/www1/groups/webassets/@marketing-public/documents/webcontent/transloading-feb2015-wp.pdf

rail operators move the customer's freight near the final delivery point, with contracted trucking companies completing the final mile. However, this method of cargo distribution has been recently challenged, with critics arguing the method results in sub-optimal cargo loads and inefficiencies due to the requirement for cargo to be funneled through off-site distribution centers.

Landlord port security came about after the terrorist attacks of 9/11. New rules called for mandated vessel inventories, security plans and assessments as well as screening procedures for both passengers and cargo. The security of U.S. ports is under the jurisdiction of the United States Coast Guard (USCG) as part of the International Port Security Program (ISP). This is done with the use of International Port Security Liaison Officer (IPSLO), according to the USCG website.[6] The USCG does not only manage the security of ports locally, they work with international ports as well through reciprocal agree with port that the U.S. does business with [7]. The majority of ports around the world if not all of them work under two organizations that govern how these ports operate internationally. The first is the International Maritime Organization (IMO) and the second is the International Ship and Port Facility Security Code (ISPS)[8]. U.S. Code Title 46, Subtitle VII, Chapter 701, and Subchapter I is the main reference for determining who has the legal authority or mandate to provide port security.[9]

Challenges and Issues:

It is critical to remember that a port is a border. Therefore, the federal government has a key role in port security. The Customs agency in each country generally works to protect the country by detecting unauthorized goods and securing the

[6] United States Coast Guard; U.S. Department of Homeland Security: Web site 09/08/2015 http://www.uscg.mil/d14/feact/Maritime_Security.asp
[7] Ibid
[8] Ibid
[9] Legal Information Institute [LLI], (1992), Cornell University Law School, Retrieved from: https://www.law.cornell.edu/uscode/text/46/41302

border; by working with fiscal revenues to ensure adequate valuation of goods; and by facilitating legitimate trade.[10] Therefore, Customs in most countries is involved in port security. In the United States, this agency is known as the Customs and Border Protection (CBP). The most prominent threat to ports in the United States is the possibility of a terrorist attack. Given the sheer volume of shipping containers pumped in and out of U.S. ports per day, it is no wonder why this is such a concern. The CBP, Coast Guard, and the Transportation Security Administration (TSA) work with other federal agencies and state and local agencies to combat this constant threat. The security of ports will undoubtedly continue to evolve to face the ever-changing threats to the homeland of the U.S.

It is no secret that terrorist want to impose destruction on the U.S., for this reason security planners constantly research new ways to decrease Americas susceptibility to harm on our homeland. This holds true for ports in the private sector as well. The challenge for authorities not figuring out where a threat may arise from, the issue lies in figuring out what kind of a potential attack may occur on the ports, and how to effectively manage security without much funding. It is very essential to protect and guard our maritime ports due to their vulnerability and vital role in our nation's economy. It is mentioned over and over that communication between the government and private sector stakeholders must be improved. In the past few years, our nation has improved intelligence aptitude dramatically since 9/11. Threats to maritime transportation continue to evolve though. Everything from weakness in infrastructure to ship security itself must be looked at and examined in order to implement best practices in securing the ports. Many feel today interagency security is lacking when it comes to effectively managing

[10] Juhel, M. H. (2010). Management Models and Public/Private Partnerships in the Port Sector. *The World Bank*. Retrieved from http://www.icafrica.org/fileadmin/documents/ICA_sponsored_events/IFC_PPP_Ports_Cairo_2010/Management%20Models%20and%20PPPs%20in%20the%20Port%20Sector%20MJuhel.pdf

and securing private ports because security is often left up to local authorities and the Coast Guard. Improving security within private sector ports focuses on cross-governmental multi-agency collaboration that drives policy formulation and execution. However, many will argue that the private sector should not enjoy the benefits of being protected by the government. Often government officials disagree on the role that interagency should play when it comes to protecting these ports due to the fact there is no centralized coordinating mechanism.[11]

Ports throughout the United States operate with different levels of security. The Port of Los Angeles has its own Los Angeles Port Police, who are the immediate responders and secure the property and traffic flow in and out of the port on land. The U.S. Coast guard is on site as well as Customs and Border Protection of DHS.[12] Within the Port of Los Angeles, private agencies coordinate the paperwork and acceptance of freight, ensuring that it is within the protocol of U.S. Homeland Security regulations. Although these are primarily private agencies they are licensed through the local custom authority. The Coast Guard has a significant role in protecting the waters around our nation, but the Customs and Border Patrol branch of DHS provides security for a reported 328 land, air, and seaports.[13] Other ports such as Long Beach and New York operate in similar manners. As the port size begins to get smaller, so do the resources. One can see from the official websites of the Oakland Port and Savannah Port that there is not a significant amount of information on the security agencies involved on site. One report

[11] Chapman, L., & OF THE, N. S. (2004, Jan 03). Maine on target with port security private sector ready for strict new rules. *Bangor Daily News* Retrieved from http://search.proquest.com/docview/414163135?accountid=7398\
[12] *Port of Los Angeles, City of Los Angeles*. (2015, September 23). Retrieved from Port of Los Angeles: https://www.portoflosangeles.org/
[13] US Department of Homeland Security. (2015, October 1). *At Ports of Entry*. Retrieved from US Customs and Border Patrol: http://www.cbp.gov/border-security/ports-entry

details the increased spending on port security throughout the nation.[14] These costs are on the rise because of technological advances.

Current Actions Taken to Mitigate the Issues or Challenges:

With the majority of business being handled by private organizations, the public sector must be concerned with regulations and policy to safeguard the port and the homeland. When it comes to the security of U.S. ports and all transient cargo and personnel, the buck stops with DHS. The DHS has the overall task of overseeing and ensuring port security by working with the other agencies and continuing to find ways to protect the United States.[15]

As mentioned, one of, if not the greatest challenge for port security is countering the constant, ever-evolving threat. This challenge, along with the several other challenges and issues mentioned have been frequently addressed by DHS and by other federal, state, and local port stakeholders (public and private sectors), through numerous programs and security initiatives. The DHS has three primary agencies that have implemented the most significant programs. First, the USCG introduced regulations and programs that require ports, port related facilities, and port operators to address security issues within their individual entities. The requirements entailed that the public and private sector actors must develop, introduce, and maintain individual organization security plans within their respective organization to identify and address their susceptibilities so to mitigate these issues.[16] These individual assessments and security plans are required to be performed regularly to ensure that vulnerabilities are identified

[14] Pate, A., Taylor, B., & Kubu, B. (2008). *Protecting America's Ports: Promising Practices.* US Department of Justice.
[15] GAO-14-636T: *Maritime security: Progress and challenges with selected port security programs before the committee on Homeland Security and Governmental Affairs*, U.S.Sen.1 (2014) (Testimony of Stephen Caldwell). Retrieved from http://wwwgao.gov/products/GAO-14-636T.
[16] GAO-14-636T

and address, as well as communicated cross-sector, to identify weaknesses and potential risks and mitigate against the threat.

A significant challenge remains, however, in the unavoidable dependence upon security efforts at foreign ports of origin. This requires diplomatic and DHS partnership with counterparts overseas.[17] The CBP provides security in a layered approach, focused on identifying and/or mitigating potential threats to the port, more generally to the safety and security of the homeland. The CBP does this by providing a presence at foreign ports and having foreign-based inspectors to inspect cargo that is US-bound.[18] The CBP is also responsible for inspecting cargo arriving in the U.S. Since the CBP is widespread and very active around the globe, it offers unique opportunities for them to develop partnerships and collaborate with foreign Custom agencies and private businesses around the globe to provide security to the global supply chain and security at home. The CBP has accomplished this through two notable program, the first being the Container Security Initiative (CSI). The CSI is an action taken by the CBP to establish a presence at various ports around the globe, to work with and develop partnerships within the trade community.[19] This allows the CBP to gather intelligence and determine potential risks of cargo shipments before the shipment arrives in the US. The CSI program was initiated by the CBP to enable the capabilities for advance screening on cargo before it is loaded onto ships set for the US.[20] The second significant program of the CBP that utilizes international partnerships with private sector organizations is the Customs-Trade

---

[17] GAO-14-636T: *Maritime security: Progress and challenges with selected port security programs before the committee on Homeland Security and Governmental Affairs*, U.S.Sen.1 (2014) (Testimony of Stephen Caldwell). Retrieved from http://wwwgao.gov/products/GAO-14-636T.

[18] RAND: Center for Terrorism Risk Management Policy. (2006). *Center for Terrorism Risk Management Policy*. Retrieved September 29, 2015, from RAND: http://www.rand.org/content/dam/rand/pubs/monographs/2006/RAND_MG520.pdf

[19] Department of Homeland Security. (2015). *U.S. Customs and Border Protection*. Retrieved from http://www.cbp.gov/border-security/

[20] CT410: *Securing America's ports: Testimony before the Committee on Homeland Security and Governmental Affairs*, U.S.Sen.1 (2014) (Testimony of Henry Willis). Retrieved from http://www.rand.org/pubs/testimonies/CT410.

Partnership against Terrorism (C-TPAT) program. The C-TPAT is a voluntary program enabling the CBP and the private sector companies to work in unison to provide security of the supply chain.[21] The C-TPAT initiated by the CBP is geared towards securing the supply chain, while mitigating the impact of new security measures on free market trade.[22]

The last primary Federal level agency is the Transportation Security Administration (TSA). The TSA provides security measures in the form of surveillance systems and programs.[23] Specifically, the TSA administers a credentialing system that heightens security in secure cargo areas. The system, coined as the Transportation Worker Identification Credentialing (TWIC), works by biometrically verifying personnel so that only authorized individuals gain access to maritime ports and areas within these ports.[24]

Recommendations for Improving Best Practices:

One of the key issues and struggles regarding port security is how to integrate and incorporate the private sector. A project done by the Council of Foreign Relations aimed at determining issues between private and public sector securities of port infrastructures determined that the private sector was willing and able to play a larger role in providing security, but the federal government made it difficult for them to do so[25]. Post 9/11 reorganizations in the federal government was one of the difficulties along with lack of

[21] GAO-14-636T: *Maritime security: Progress and challenges with selected port security programs before the committee on Homeland Security and Governmental Affairs*, U.S.Sen.1 (2014) (Testimony of Stephen Caldwell). Retrieved from http://wwwgao.gov/products/GAO-14-636T.
[22] CT410: *Securing America's ports: Testimony before the Committee on Homeland Security and Governmental Affairs*, U.S.Sen.1 (2014) (Testimony of Henry Willis). Retrieved from http://www.rand.org/pubs/testimonies/CT410.
[23] *Port of Los Angeles, City of Los Angeles*. (2015, September 23). Retrieved from Port of Los Angeles: https://www.portoflosangeles.org/
[24] Sadler, S. (2013, June 18). *Testimony on TSA's role in the Transportation Worker Identification Credential (TWIC) program.* Retrieved September 29, 2015, from Official website of the Department of Homeland Security: TSA: https://www.tsa.gov/news/testimony/2013/06/18/testimony-tsas-role-transportation-worker-identification-credential-twic
[25] Flynn, S & Pricto, D. (2006, April 28). Capitalizing on the Private Sector to Protect the Homeland. Retrieved from http://www.cfr.org/border-and-port-security/capitalizing-private-sector-protect-homeland/p10560

information sharing to the private sector, lack of funding and lack of preparation for major disasters.

One key thing to point out is to make sure that the CEO's and other heads of private companies understand that the final say on how to protect ports and their infrastructure is the responsibility falls on the federal government which does not give that CEO the final say on how to go about protecting the port. With that being said, it is also very important for the federal government to constantly evaluate and improve individual ports, not using general evaluations and counting on blanket recommendations to work for all ports when clearly all ports have their own special needs in regards to security and what they are protecting from and against. It is imperative that there be an increase in information sharing between the private and public sector regarding pertinent safety bulletins.[26]

The continuing concerns of stowaways, especially those coming from affected areas with issues like Ebola, is a major law enforcement concern that can be made easier and help lessen the burden by including the private sector in the screening process at foreign ports as well as clearing operations here at our ports. This threat could end up being an issue that needs pushed up the chain up to and including the need for new legislation being introduced to flag ships coming from these areas.

The public sector can also do a better job of working with the private sector when it comes to implanting security guards and protocols, starting with hiring processes all the way through offering employment and training as well as continuing education. Another key factor to consider is following (and expanding into the private sector) the lead of the Jacksonville Port Authority (JAXPORT) in regards to implementing P25 compliant radio

[26] Flynn, S & Pricto, D. (2006, April 28). Capitalizing on the Private Sector to Protect the Homeland. Retrieved from http://www.cfr.org/border-and-port-security/capitalizing-private-sector-protect-homeland/p10560

systems that allow the port to communicate with local officers. Allowing the private sector to access the P25 system would allow a better means of communication between everyone working at the port and allow for one standard way of radio communication and the ability for private sector security to immediately contact and communicate with the public sector in regards to the public safety radio system.

Incorporating and allowing the private sector to assist with port security will add flexibility to what the ports are already doing to secure and protect from the main issues that they face; smuggling, human trafficking, drug trafficking or even acts of terrorism. Private investment is contributing significantly to modernization efforts for trans-loading cargo and port security as a whole.

With the lack of funding that faces the public sector, incorporating the aforementioned ready and willing private sector is a must. With that comes the demand for better communication between the government and both private and public port security. Similar to the issues that were exposed after 9/11, many still feel today that interagency security is lacking when it comes to effectively managing and securing ports due to the differences facing federal authorities like the United States Coast Guard and local authorities. Improving security within private sector ports focuses on cross-governmental multi-agency collaboration that drives policy formulation and execution, and bringing all the players, federal, state, local and private, to the table to come together will benefit all parties involved in securing our ports.

"Private Sector Elimination of Criminal Activity and Security Gaps"

Catherine Dutton
Graduate Certificate in Homeland Security & Emergency Management
Expected Graduation: December 2016

Aaron Fields
Graduate Certificate in Homeland Security & Emergency Management
Expected Graduation: December 2016

Leia Foster
Graduate Certificate in Homeland Security & Emergency Management
Expected Graduation: May 2016

Katharine Heinz
Master of Science in Criminal Justice & Public Safety
Expected Graduation: May 2017

Indiana University School of Public and Environmental Affairs
Indiana University – Purdue University Indianapolis

Situation:

In a general sense, most private sector organizations identify criminal activity and security gaps within their respective organizations both by way of the risk management process and/or the security officials each has established/enlisted to protect their individual interests and assets. The methodology and system tends to vary from organization to organization in the private sector; however, nearly all private entities or organizations adhere to/have in place some form and varying degree of a systematic risk management process to provide protection and security to their business. Mostly private security professionals and/or security personnel within the individual organization run these risk management systems for each individual organization. The practices and methods used by each individual organization vary, as previously stated, but the duties fall on and the process itself is carried out in either one of two common ways or in some cases a combination of both – i.e., internal and/or external security personnel.

Internal security consists of selected or hired personnel from within an individual organization tasked specifically with running the risk management system and following through and implementing the security practices and protocols in place. External security usually consists of security professionals and/or private security firms hired or consulted to establish and/or operate the security system for an organization – i.e., third-party security professionals. As alluded, an organization's security process is managed and operated either internally or externally, or in some cases the internal security management consults or outsources specific duties to a third-party external security source.

Challenges and Issues:

The private sector's risk management process is quite similar to that used in the public sector. The process is largely driven by crime analysis and= it is common practice for private organizations to implement and follow broad guidelines and protocols established by industry associations.[1] The risk management security system is set up to mitigate, prevent, respond, and recover from any perceived, imminent, ongoing, or carried out threat or act. Thus, identifying criminal activity within the confines of the organization falls within the risk management process. The private sector does this by applying or during a standard or specific threat/risk assessment of its organization or its supply chain. This process is done by utilizing law enforcement data and/or by conducting and/or reviewing in-house security reports.[2] By conducting a crime analysis, the organization uses data collected by law enforcement agencies – local,

[1] Vellani, K. H. (2010). *Crime analysis for problem solving security professionals in 25 small steps.* Center for Problem-Oriented Policing. Retrieved from http://www.popcenter.org/library/reading/pdfs/crimeanalysis25steps.pdf

[2] Vellani, K. H. (2010). *Crime analysis for problem solving security professionals in 25 small steps.* Center for Problem-Oriented Policing. Retrieved from http://www.popcenter.org/library/reading/pdfs/crimeanalysis25steps.pdf

state, tribal, federal agencies – to identify and link common crime trends or methods of operations (MOs) of criminals in general or specific to the area or industry of the organization.

By identifying these trends and MOs, an organization's security management and personnel can zone in on specific threats to specific sections or assets of their organization or focus on specific vulnerabilities of their organization and/or supply chain. This enables the organization to identify areas at risk, look into those areas – whether they be in the security itself, employees or personnel most at risk to be taken advantage of, or assets criminals may target or utilize to carry out their crime – and either find security gaps within the confines of their organization or identify discrepancies or suspicious activity and determine if they are in fact actual criminal activities. Businesses in the United States have a long history of collaboration and cooperation with the public sector on security matters. However, until recently, legal restrictions prevented companies from influencing social affairs.[3] With the removal of these restrictions in the 1950s, corporations began looking to "cultivate a broad view of their own self-interest while instinctively searching for ways to align self-interest with the larger good."

Businesses have strong economic incentive to contribute to homeland security programs to prevent criminal and/or terrorist disruptions to their operations and disaster response efforts to return to normal operations as expeditiously as possible post-incident.[4] Through programs such as the Customs-Trade Partnership Against Terrorism (C-TPAT), the private sector is better able to integrate into the wider customs and border protection architecture. C-TPAT offers significant financial incentives for private sector

---

[3] Smith, N. C. (1994). The New Corporate Philanthropy. *Harvard Business Review* (May-June), Pg. 106-116.

[4] Young, D. Y., & Burlingame, D. F. (1996). Paradigm Lost: Research toward a New Understanding of Corporate Philanthropy. In D. Y. Young, & D. F. Burlingame, *Corporate Philanthropy at the Crossroads* (pp. 158-176). Bloomington: Indiana University Press.

port industry cooperation such as reduced examination rates for importers, expedited border crossing privileges and 'front of the line' customs processing.[5] Over 10,000 firms are certified through C-TPAT and work closely with United States Customs and Border Protection on port security issues.

Technology plays an increasingly important role in the implementation of both private and non-private port security. CCTV cameras and motion detectors have been used in ports for several decades. The port security industry has had to keep up with the shift towards the digital world. Much of the advances have been done in the area of surveillance. Large companies like *Controp* provide surveillance equipment such as High performance Stabilized Observation Payloads used for day and night surveillance on board: UAVs, helicopters, VTOLs, light aircraft, maritime boats, USVs, ground vehicles and UGVs.[6] These advanced devices make it possible for a smaller staff, made up of employees who may or may not have formal law-enforcement training to provide adequate surveillance over the large areas which ports naturally entail. Ports have also implemented technology driven security features involving radar sensors, sonar sensors, integrated GPS and GIS mapping systems, and electronic card readers for access control. These advancements have become part of the framework which makes up port security, and relies on the relationship between private businesses, the ports, and the local, state, & federal law enforcement. This inter-agency multi-dimensional approach to security has required the responsible entities to redesign and rewrite their standard operating procedures

<u>Recommendations and Best Practices:</u>

---

[5] U.S. Customs and Border Protection. (2014, January). *C-TPAT Program Benefits: Reference Guide.* Retrieved October 16, 2015, from Customs-Trade Partnership Against Terrorism: https://www.cbp.gov/sites/default/files/documents/C-TPAT%20Program%20Benefits%20Guide.pdf

[6] Controp.com. (2015). from http://www.controp.com/category/company-profile/ Retrieved 16 October 2015.

Identifying security gaps and responding effectively presents a complex challenge requiring a well-coordinated whole-of-community effort. Many academic reviews and case studies suggest that private-public port security collaboration has the potential to reduce security costs and improve the overall effectiveness of port security operations. A number of authors such as Sheffi insist on a joint collaboration of the private and the public sector, which can increase the supply chain security of all ports.[7] Port security should extend to certain parameters in security namely:

1. Neutralizing vulnerabilities for criminal activity within the port,
2. Identifying and responding to safety issues,
3. Minimizing the threat of terrorism,
4. And sharing intelligence and investigative information with appropriate law enforcement agencies.[8]

Writers for The Journal of the NPS Center for the Homeland point out: "Public-private partnerships are a major issue of discussion in businesses and government agencies concerned with homeland security… America's ports are vital hubs of economic activity."[9] The authors continue to identify pre-existing programs such as the Customs Trade Partnership Against Terrorism program (C-TPAT), the Transportation Worker Identification Credential program (TWIC), the Screening Partnership Program (SPP) in airports, and the many technologies and equipment made by the private sector to make the public sector's job easier.

---

[7] Sheffi, Y. (2001). Supply chain management under the threat of international terrorism. *The International Journal of Logistics Management , 12(2)*, 1-11.

[8] Christopher, Kenneth. (2015). *Port Security Management: Second Edition*. Boca Raton: Taylor and Francis Group.

[9] Busch, N. E., & Givens, A. D. (2012). Private-Public Partnerships in Homeland Security: Opportunities and Challenges. *Homeland Security Affairs , 8*.

Marine terminal operators (MTO) are the private sector companies operating terminal facilities within ports under direction of the overall port authority line.[10] The challenge for MTOs is to put into place effective security measures while maintaining efficient and cost effective port operations. While no ports are exactly identical, many share certain vulnerability characteristics. Due to the size of most ports, the inherent accessibility makes it difficult to apply effective security measures. Additionally, the sheer amount of material being transported provides a ready avenue for the introduction of different types of threats.[11]

Terminal operators are required to maintain security for the property leased from the port authority.[12] The U.S. Coast Guard and Customs and Border Patrol (CBP) set minimum requirements for marine terminal operators' security programs. Frittelli, describes the basic elements of the security programs and at the heart of these programs is the terminal operator's security assessment and facility security plan. The plan requires operators to address gaps identified in the assessment, specify methods to restrict access to the terminal, identify methods to monitor terminal activities through security guards, alarm systems, water patrols, surveillance equipment and lighting, procedures for checking container seals, and

---

[10] Frittelli, J. F., & Lake, J. E. (2006). *Terminal Operators and Their Role in U.S. Port and Maritime Security*. Washington DC: CRS Report for Congress.

[11] Hecker, J. Z. (2002, August 5). *Nation Faces Formidable Challenges in Making New Initiatives Successful.* Retrieved November 26, 2015, from United States General Accounting Office.

[12] Frittelli, J. F., & Lake, J. E. (2006). *Terminal Operators and Their Role in U.S. Port and Maritime Security*. Washington DC: CRS Report for Congress.

verifying that arriving trucks and workers have legitimate business at the facility. Terminal operators work closely with the CBP to provide for container movement necessary to facilitate their inspections. As part of

the security plan, the terminal operator must designate a Facility Security Officer (FSO) as the single point of contact for security and communications to the Coast Guard and CBP. The FSO is required to conduct on site security exercises, drills, and assessments to determine gaps within a private sector operator's security program. These internal security assessments and drills are a key activity conducted by terminal operators to improve systems and procedures. Increasing the frequency and involving third-party security experts presents an opportunity to improve the process.

The private sector terminal operator is responsible for not only its own labor force but also for a wide variety of transportation workers, contractors, visitors, and temporary workers that enter terminal property. Individuals entering the terminal must either be fully escorted are possess a Transportation Workers Identification Credential (TWIC). The TWIC prescreens individuals with a background check and identifies the individual with a photograph and biometric data, including fingerprints. The terminal operator is responsible for verifying the TWIC credentials for all unescorted individuals on terminal property. Terminal operators can improve the TWIC process by updating card reader technology used at terminal access points to verify credentials, biometric data (fingerprints) and match the individual with database records. This represents a significant security improvement over the practice of simple visual verification of the workers identification card.

In order for port security to be enhanced in maritime ports by the private sector, more incentives and possibly even mandatory regulations passed by Congress to promote enrollment and compliance in programs such as these. While programs like TWIC and C-TPAT help to form an understanding between the Federal government and private sector businesses, government must be weary of letting trust take the

place of security. Some of these programs allow for added trust to the point that cargo may not be checked as thoroughly from a trusted vendor. This should be done very lightly to ensure security is met, all the while

private sector organizations must conform to preparatory and operational measures to ensure the secure U.S. homeland.

Ports throughout the United States operate with different levels of security, generally based on the size of their operations. Some ports use a combination of private sector security companies working alongside sworn officers of state and federal authorizations. Private sector security has grown substantially across the world to a point that private security officers out number public sector law enforcement by more than three to one.[13] Private security has been able to adopt new technologies and techniques much faster than public departments.[14] While private security is alluring due to realized cost savings, it does pose some issues. Private services do not have the same legal authority as sworn officers and may need to rely on local law enforcement to make an arrest. Private security companies must train employees on probable cause and proper evidence gathering to effectively detain individuals or groups. There can be a large gap in training between government agencies and the private industry. Working alongside or under a law enforcement agency can enhance the effectiveness of private security organizations. In 2011, private

---

[13] Blackstone, E. A., & Hakim, S. (2013). Competition versus monopoly in the provision of police. *Security Journal , 26 (2)*, 157-179.

[14] Blackstone, E. A., & Hakim, S. (2013). Competition versus monopoly in the provision of police. *Security Journal , 26 (2)*, 157-179.

security firm Allied Barton assisted a south Florida port with transitioning to a hybrid port security model from full law enforcement to a combination of contract security and law enforcement officers.[15] The port

successfully reduced security costs while maintaining a high level of protection through collaboration amongst the local County Sheriff's Office and the private security firm. The research urges ports to collaborate with reputable private security firms who maintain high levels of training and certification. This research suggests the Department of Homeland Security and the United States Coast Guard should investigate creating a standard training curriculum and level of certification for private security firms wishing to operate as hybrid security model or a fully privatized port security model. Additionally, according to a report by the U.S. Congressional Budget Office, "businesses would be inclined to spend less on security than might be appropriate for the nation as a whole if they faced losses from an attack that would be less than the overall losses for society."[16] To incentivize the private sector to increase security practices and spending, the Center for American Progress suggests government intervention and regulation. They suggest three options to engage and enforce increased security practices: impose standards requiring the private sector to meet a set of security standards; government can provide direct subsidies and/or

---

[15] Allied Barton. (2015). *AlliedBarton Collaborates with Sheriff's Office to Secure Port Together*. Retrieved November 26, 2015, from Allied Barton: http://www.alliedbarton.com/Security-Resource-Center/Case-Studies/View-Case-Study/ArticleId/286/AlliedBarton-Collaborates-with-Sheriff-s-Office-to-Secure-Port-Together

[16] US Congressional Budget Office . (2004, December). *Homeland Security and the Private Sector*. Retrieved November 26, 2015, from US Congressional Budget Office: http://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/60xx/doc6042/12-20-homelandsecurity.pdf

incentives to offset the costs of increased security measures; and establish market based measures enabling companies to more efficiently allocate resources.[17]

It is essential to ensure there is effective communication links between private port operators, private port security firms and the government security apparatus. Collective information and information exchange in times of emergency or terrorism related issues should be effective and succinct. The new changes in the National Terrorism Advisory System (NTAS) was designed by US government to "improve capabilities and effectiveness of the federal government in communicating information about terrorist threats to public, government agencies, first responders, airports and other transportation and private sectors."[18] Forming a database system that shares information with the private sector ports and government agencies is paramount. The database should be limited to a need-to-know only basis and should be also accessible by certain elected officials and verified private security employees within the system. In case of emergency situations, the database should be formatted in an orderly fashion to deal with information overload issues and provide specific contextual information. In addition, a national policy should be encouraged to improve links between both sectors. Furthermore, many ports rely on employee diligence and self-reporting of security issues. This method of security could be improved by implementing

---

[17] Housman, R., & Olsom, T. (2005). *New Strategies to Protect American: A Market-Based Approach to Private Sector Security*. Retrieved November 27, 2015, from The Center for American Progress: https://www.americanprogress.org/wp-content/uploads/kf/FECREPORT.PDF

[18] Christopher, Kenneth. (2015). *Port Security Management: Second Edition*. Boca Raton: Taylor and Francis Group.

incentive programs and protections for whistleblowers that report everything from security vulnerabilities to corporate fraud to theft.[19]

[19] Busch, N. E., & Givens, A. D. (2012). Private-Public Partnerships in Homeland Security: Opportunities and Challenges. *Homeland Security Affairs , 8*

"Private Sector Engagement and Public-Private Coordination in Port Security"

Terrice Hooks
Graduate Certificate in Homeland Security & Emergency Management
Expected Graduation: May 2016

Lauren Kenney
Master of Science in Criminal Justice & Public Safety, Graduate Certificate in Homeland Security & Emergency Management
Expected Graduation: May 2017

Beau Parker
Graduate Certificate in Homeland Security & Emergency Management
Expected Graduation: May 2016

Indiana University School of Public and Environmental Affairs
Indiana University – Purdue University Indianapolis

Situation

The 9/11 Commission estimated that the private sector owns and protects 85% of the nation's infrastructure.[1] The U.S. government recognizes the need to have the private sector engaged in port security procedures. There is a wealth of knowledge, experience, and resources provided by the private sector, making their partnership with government at various levels invaluable when it comes to improving and enhancing port security procedures.

Multiple initiatives have been implemented by port security agencies to incorporate the private sector in port security procedures. "Public-private partnerships have been defined as collaboration between a public sector (government) entity and a private sector (for-profit) entity to achieve a specific goal or set of objectives."[2] These private sector entities are often able to help fulfill the security needs of public sector ports through less expensive and more effective

[1] 9/11 Commission. (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Official Government Edition. Washington, DC: U.S. Government Printing Office.
[2] Busch, Nathan E., and Austen D. Givens. (2012, October). Public-Private Partnerships in Homeland Security: Opportunities and Challenges. *The Journal of the NPS Center for Homeland Defense and Security*. Retrieved from https://www.hsaj.org/articles/233

means. "Where the public sector is hard pressed to effectively address the monumental task of protecting ports and the through movement of people and cargo, industrious private firms have stepped up, developing, testing, marketing and implementing new products and services that are helping transportation providers and ports, and all those concerned with their protection."[3]

Public-private partnership is essential to facilitate security to the homeland, and thus, is an integral part to maritime port operations. History has taught the United States government that the emergency management cycle, homeland security, and even military/defense endeavors are reliant on the private sector in order to be successful. A few of these historical events that have bridged the inevitable partnership are the Great Chicago Fire of 1871, the 1906 San Francisco Earthquake, World War II, the Cold War, 9/11/2001, Hurricane Katrina, and the Deepwater Horizon incident—just to name a few highlighting events.[4] In the wake of these devastating events to the country, private organizations played a pivotal role in sustaining the government's efforts—everything from citizens participating in civil defense and private military manufacturing, to charitable contributions in recovery, and to fishermen assisting in cleanup efforts. All of these demonstrate the much needed cooperation the public sector must have with the private sector. Inversely, in times past, and even more so today, the private sector relies on this partnership to protect their internal supply-chain and economic stability. Without governmental safeguard, the market, as well as goods and services, can become targets for the enemy.

Challenges and Issues

[3] Musser, Lori. (2012, December 11). Strong Seaports- Teaming Up to Step Up Safety and Security. *AAPA Seaports.*
[4] Busch, N. E., & Givens, A. D. (2012, October). *Public-Private Partnerships in Homeland Security: Opportunities and Challenges*. Retrieved October 2015, 2015, from Homeland Security Affairs: https://www.hsaj.org/articles/233

A key point for security throughout U.S. ports is identifying gaps. To identify gaps the organization must be continually performing security self-assessments.[5] Unfortunately, this is not always done in every port throughout the nation. Ports still pose a significant risk due to the sheer volume of cargo and individuals that pass through each and every day.

So what is it that is contesting the U.S. ports? What are the threats, challenges, and dangers posed to the U.S. through maritime port security breaches? The primary entities in ports comprise personnel, goods, and funding. The majority of goods are transported in containers which could be exploited not only by illegitimate good transporters, but also by hijacked vessels that appear to be friendly. Stuart Flynn refers to this potential terrorist threat as a "Trojan Horse" vessel.[6] The other threat is the personnel—the individuals securing ports as well as the business people and their laborers taking advantage of the economic opportunities that lie there.

There are other more modern threats that have emerged with the advent of a steadily all-time high national debt and contemporary logistics and operations relying heavily on the cyber realm. The funding for port security has been deemed as "grossly underfunded" – being cited to having received lower funding over a six year period than funding for the Iraq war received over a 2 and a half hour span.[7] The other contemporary concern is that of cyber security. With cyberterrorism and cyberwarfare growing National Security concerns, it should be no surprise maritime ports are at risk here as well. Compromise of maritime port cyber-prone elements

[5] Harrison, E. (2011, January). *Securing the Supply Chain*. Inbound Logistics. Retrieved from http://www.inboundlogistics.com/cms/article/securing-the-supply-chain/

[6] Flynn, S. (n.d.). *Port Technology Web site: Assessing and confronting the challenges of port security.* Retrieved from Excerpt from Port Technology International's Edition 40: https://www.porttechnology.org/technical_papers/assessing_and_confronting_the_challenges_of_port_security/

[7] Flynn, S. (n.d.). *Port Technology Web site: Assessing and confronting the challenges of port security.* Retrieved from Excerpt from Port Technology International's Edition 40: https://www.porttechnology.org/technical_papers/assessing_and_confronting_the_challenges_of_port_security/

include control systems, vessel networks, tracking technology, and logics software.[8] If any of these items are affected it could make vulnerable ports more prone to physical attacks; but it also could cause severe economic blows due to port operations being delayed and impacted.

Current Actions Taken to Mitigate Challenges and Issues

At the federal level, there are several initiatives in place to gain private sector involvement in port security procedures. The Customs Trade Partnership Against Terrorism (C-TPAT) is "a government-business sector initiative that was created to enhance worldwide supply chain security. Over 10,000 firms are certified through the C-TPAT program, meaning they enjoy close working relationships with United States Customs and Border Protection (CBP), are able to obtain government risk assessments of their supply chain, and can attend special government-sponsored supply chain security training sessions." It is programs such as C-TPAT that help to provide a broad administrative framework for public-private sector coordination.[9]

Section 109 of the Maritime Transportation Security Act of 2002 required the Secretary of Transportation to "develop standards and curriculum to allow for the training and certification of maritime security professionals."[10] The responsibility for providing the curriculum was delegated to the United States Maritime Administration, who in turn utilized the U.S. Merchant Marine Academy to develop and deploy training programs. According to MARAD, "The goal of this voluntary certification program is to promote high quality, uniform training of maritime

[8] Walters, R. (2015, February 23). *Issue Brief on Homeland Security: The U.S. Needs to Secure Maritime Ports by Securing Network Ports.* Retrieved from The Heritage Foundation Web site: http://www.heritage.org/research/reports/2015/02/the-us-needs-to-secure-maritime-ports-by-securing-network-ports

[9] Busch, Nathan E., and Austen D. Givens. (2012, October). *Public-Private Partnerships in Homeland Security: Opportunities and Challenges. Homeland Security Affairs* 8, Article 18. Retrieved from https://www.hsaj.org/articles/233

[10] United States Marine Administration. *Maritime Transportation Security Act (MTSA) Course Certification.* (n.d.). United States Maritime Administration, United States Department of Transportation. Retrieved from http://www.marad.dot.gov/education/maritime-transportation-security-act-mtsa-course-certification/.

security professionals."[11] The curriculum includes six distinct courses, five of which have direct application for private sector port security personnel. Courses are provided for specific personnel, including; the Company Security Officer, the Facility Security Officer, Vessel Personnel with Security Duties, and Facility Personnel with Security Duties. The curriculum also includes an awareness level course in maritime security. Over 17,000 maritime security personnel have attended one or more of the courses.

The Transportation Worker Identification Credential (TWIC) program works to enhance private sector involvement in port security. The TWIC program "pre-screens workers with unescorted access to sensitive areas of America's ports to ensure they do not pose a security threat." This helps to further supply chain security and also pushes to achieve port security objectives.[12]

The Federal Emergency Management Agency (FEMA)'s annual Port Security Grant Program (PGSP) is one such endeavor to incentivize the private sector when it comes to enhancing port security. The PGSP is one of FEMA's grant programs that directly supports maritime transportation infrastructure security activities. On the PGSP webpage, FEMA notes:

> The vast majority of U.S. maritime critical infrastructure is owned and operated by state, local, and private sector maritime industry partners. PSGP funds available to these entities are intended to improve port-wide maritime security risk management; enhance maritime domain awareness; support maritime security training and exercises; and to maintain or reestablish maritime security mitigation protocols that support port recovery and resiliency capabilities. PSGP investments must address Coast Guard identified vulnerabilities in port security and support the prevention, detection, response, and/or recovery from attacks involving improvised explosive devices (IED) and other non-conventional

[11] United States Maritime Administration. *Maritime Transportation Security Act (MTSA) Course Certification*. (n.d.). United States Maritime Administration, United States Department of Transportation. Retrieved from http://www.marad.dot.gov/education/maritime-transportation-security-act-mtsa-course-certification/.
[12] Busch, Nathan E., and Austen D. Givens. (2012, October). *Public-Private Partnerships in Homeland Security: Opportunities and Challenges. Homeland Security Affairs* 8, Article 18. Retrieved from https://www.hsaj.org/articles/233

weapons.[13]

Eligible applicants to the PGSP are those who deal with the implementation of Area Maritime Security Plans (AMSP) and Facility Security Plans (FSP) among port authorities, facility operators, and state and local government agencies that are required to provide port security services. This is done under the authority of the Maritime Transportation Security Act of 2002.[14] By hosting such a program, FEMA is encouraging the private sector to get involved in port security procedures and incentivizing them to come up with innovative solutions to port security needs.

Other initiatives, such as CBP's Consolidation Appropriations Act, allow for the private sector to appropriate and essentially donate resources to the agency.[15] This type of cooperation saves the public sector money and benefits the private agency through the building of trust, tax write offs, and by putting resources to good use. Additionally, to aid in the incorporation of the private sector in port security, the U.S. Department of Justice launched "Operation Cooperation"—a national effort to increase collaboration between the private sector, particularly private security and state and local law enforcement agencies.[16] As part of the operation, a guidelines document was created that focused on how the public and private sector could pool their resources to reduce crime and public disorder.

---

[13] Federal Emergency Management Agency. (2015, July 28). *Fiscal Year 2015 Port Security Grant Program.* FEMA, U.S. Department of Homeland Security. Retrieved from http://www.fema.gov/fiscal-year-2015-port-security-grant-program

[14] Federal Emergency Management Agency. (2015, July 28). *Fiscal Year 2015 Port Security Grant Program.* FEMA, U.S. Department of Homeland Security. Retrieved from http://www.fema.gov/fiscal-year-2015-port-security-grant-program

[15] Department of Homeland Security. (n.d.). *Public-Private Partnerships.* Retrieved October 22, 2015, from DHS Web site: http://www.cbp.gov/border-security/ports-entry/resource-opt-strategy/public-private-partnerships

[16] U.S. Department of Justice. (2003). *Engaging the Private Sector To Promote Homeland Security: Law Enforcement-Private Security Partnerships*. U.S. Department of Justice. Retrieved from https://www.ncjrs.gov/pdffiles1/bja/210678.pdf

It is easy to see the role of the federal government in coordination with the private sector regarding port security efforts, but "it is equally important for local authorities to play a part in any discussion on infrastructure protection and preparedness."[17] As the agencies on-site who possess local knowledge and relationships with key industry players, state and local agencies in port locations are an invaluable resource and contribute through various avenues. One such means is through local Area Maritime Security Committees (AMSC), which seek "to enhance communication between port stakeholders within federal, state, and local agencies, and industry to address maritime security issues."[18] Membership in an AMSC can lead to state/local law enforcement officers and even members of the private sector being granted access to pertinent national security information—if relevant to their operations and the security of their port of concern—via the State, Local, and Industry Security Clearance Program.[19] Local authorities can also coordinate with the private sector to apply for and tailor federal grant funds to meet the unique needs of their specific port of interest via the PSGP.[20] Local port authorities may coordinate with industry representatives regarding private security patrols when limited government resources prohibit the manpower necessary to provide 24/7 physical security at the port.

There are initiatives at the local and state level, but the primary coordination is linked at the federal level. Ongoing partnerships such as the Critical Infrastructure Partnership Advisory Council (CIPAC) help to foster a forum where both the public and private sector stakeholders

---

[17] U.S. Government Printing Office. (2006, June 21). *Department of Homeland Security Preparedness Grants: Risk Based or Guess Work?* Committee on Homeland Security, U.S. House of Representatives, 109 Congress, Second Session. Serial No. 109-86. Retrieved from: http://www.gpo.gov/fdsys/pkg/CHRG-109hhrg33785/html/CHRG-109hhrg33785.htm

[18] U.S. Department of Homeland Security, U.S. Coast Guard. (2015). *Area Maritime Security Committee*. Retrieved from: http://www.uscg.mil/hq/cg5/cg544/amsc.asp

[19] U.S. Department of Homeland Security, U.S. Coast Guard. (2015). *State Local and Industry Security Clearance Program (SLI)*. Retrieved from: http://www.uscg.mil/hq/cg5/cg544/sli.asp

[20] U.S. Department of Homeland Security, Federal Emergency Management Agency. (2015). *FY2015 Port Security Grant Program*. Retrieved from: http://www.fema.gov/fiscal-year-2015-port-security-grant-program

can come together to discuss security and resilience.[21] Councils such as CIPAC help to develop and implement initiatives such as TWIC and C-TPAT. These councils are imperative to public-private partnership to protect critical infrastructure, ports, and the nation as a whole.

Recommended Improvements for Best Practices

The government has many incentives in place to incorporate the private sector in port security procedures. Based on the research conducted, there are mainly federal initiatives and few local, state, and regional initiatives in place. For port security to become more efficient and effective, all levels of government must get involved with the private sector in order for ports to be as safe and secure as possible. Various branches of the federal government must consider how they can further partner with local and state governments and with the private sector.

The federal government compiled the following list of functional responsibilities via the Maritime Infrastructure Recovery Plan that the private sector may perform.

- "Participate in various maritime industry stakeholder professional organizations and advisory committees such as the AMSCs.
- Engage in exchange of information about recovery operations plans with other potentially affected private sector entities and the Federal Government to mitigate potential congestion at non-incident site ports following the diversion of vessel traffic.
- Assist in the assessment of economic impact.
- Assist in the identification of prevention and recovery resources and assets.
- Provide resources to assist in security and safety activities, as appropriate.
- Participate in pilot programs to test the effectiveness of the Federal Government to communicate security activities to the private sector.
- Using existing information-sharing mechanisms such as the National Infrastructure Coordinating Center (NICC), AMSCs, Transportation Sector Coordinating Councils and Information Sharing and Analysis Centers (ISAC), communicate situational and operational information as well as physical asset capabilities for mitigation management.

[21] Department of Homeland Security. (2015, September 17). *Critical Infrastructure Sector Partnerships*. Retrieved October 22, 2015, from DHS website: http://www.dhs.gov/critical-infrastructure-sector-partnerships

- In conjunction with Federal, state, local and Tribal authorities, assist in providing security for critical infrastructure and key resources."[22]

If the private sector works to perform these duties, they will undoubtedly contribute to a safer port security environment in the United States. The federal government should continue to find ways to incentivize the private sector to perform these duties.

Through the creation of innovative technologies, the private sector is working to meet certain unmet needs of the government when it comes to port security. For example, the SAIC Vehicle and Cargo Inspection System (VACIS) was created by a private sector business. The VACIS is "a device that emits low-level radiation, providing a rapid view of cargo containers' contents – not unlike an X-ray machine. The VACIS permits government and private sector officials to quickly evaluate if a given container poses a threat."[23] The private sector is generally very innovative when it comes to creating new technologies. Therefore, all levels of government should work to incentivize the private sector to create new technologies that will benefit port security.

The federal government should continue to fund the current programs in place; however, best practice recommends the use of evidence based practice to sustain or make appropriate changes to these programs. Even with several of these important programs underway, there are issues with them that could be solved with evidence based practice. Regarding FEMA's PGSP:

> …in 2014 FEMA stated that it is unable—due to resource constraints—to annually measure reduced vulnerability attributed to enhanced PSGP-funded security measures. Meanwhile, the Transportation Security Administration (TSA) and the Coast Guard have been administering a program requiring maritime

[22] U.S. Department of Homeland Security. (2008, April). *Small Vessel Security Strategy*. U.S. Department of Homeland Security. Retrieved from http://www.dhs.gov/xlibrary/assets/small-vessel-security-strategy.pdf
[23] Busch, Nathan E., and Austen D. Givens. (2012, October). *Public-Private Partnerships in Homeland Security: Opportunities and Challenges. Homeland Security Affairs* 8, Article 18. Retrieved from https://www.hsaj.org/articles/233

> workers to obtain a biometric identification card to gain access to certain facilities. However, in 2011, GAO recommended that DHS assess internal controls to identify actions needed to address, among other things, weaknesses governing enrollment and background checks. As of March 2014 this action had not been completed.[24]

There is a problem in the federal government of recognizing problems but not then following up and taking the appropriate steps to fix them. Therefore, operating under best practice recommendations, it is advised that each branch conducting a said program allocates the resources necessary to track the results of their program and then use this data to sustain or make changes to the program. Further assessment of the programs in place is absolutely necessary.

Some local and state officials involved in AMSCs have expressed concerned over limited government funding. Many of these agencies have had to withdraw from AMSCs because they simply cannot afford the travel and other requirements of membership. This is but one example of how a lack of funding can have a critical impact on the scope of those involved in port security. These federal programs must be continually funded so that all players are able to "come to the table" and participate.

There have been several programs implemented to improve port security and improve public-private partnerships in port security. However, there is assuredly room for great improvement. In order to effectively manage the success of the programs the government implements, more assessments of the programs must be done. There has been a great effort to improve port security through various programs and technologies, but the effectiveness of these programs and technologies has yet to be truly gauged. Only when this is done will the government grasp what changes to make and how to improve their port security endeavors.

---

[24] Caldwell, S. L. (2014, June 4). *Maritime Security: Progress and Challenges with Selected Port Security Programs*. United States Government Accountability Office. Retrieved from http://www.gao.gov/products/GAO-14-636T

"Best Practices Recommendations for Private Sector Port Security Standard Operating Procedures (SOPs)"

Christopher Lawler
Master of Science in Criminal Justice and Public Safety, Graduate Certificate in Homeland Security and Emergency Management
Expected Graduation: December 2016

Virginia Lobianco
Non-Degree Program

Adam Martin
Master of Science in Criminal Justice and Public Safety
Expected Graduation: May 2017

Rahael Mathew
Master of Science in Criminal Justice and Public Safety
Expected Graduation: December 2016

Indiana University School of Public and Environmental Affairs
Indiana University – Purdue University Indianapolis

Situation

National security assessments in the wake of the 9/11 terrorist attacks identified many shortcomings and vulnerabilities in U.S. security processes. Maritime port security emerged as one area that needed significant attention, new ideas, and more resources to bolster its defenses against criminal and terrorist threats, one aspect of efforts to make the U.S. a harder target for its enemies to penetrate. The complexity of the issue of port security has many contributing factors, including: shared responsibilities of port operation and oversight among the public and private sectors; difficulty ensuring security along the entire supply chain due to potentially lax security at foreign ports; and the sheer volume of cargo that transits U.S. ports. This study focuses primarily on the first of these factors, the need for private sector involvement in port security efforts. More specifically, the authors examine how Area Maritime Security Committees (AMSCs) and private sector entities' internal procedures impact port security. The research sought to identify challenges faced in incorporating the private sector; actions taken to-date by both the public and private sectors toward improving private sector engagement; and best practices recommended to promote greater involvement of the private sector.

Although the U.S. Coast Guard (USCG) ultimately has the lead when it comes to maritime port security in the United States, it is imperative to realize that port security is the responsibility not solely of the government, but also the private sector, which uses the ports to conduct billions of dollars in business each year at locations all along the nation's coasts and waterways. In 2002, President George W. Bush signed into effect the Maritime Transportation Security Act (MTSA). The MTSA established AMSCs "to provide a link for contingency planning, development, review, and update of Area Maritime Security Plans (AMSP), and to enhance communication between port stakeholders within federal, state and local agencies, and industry to address maritime security issues."[1]

While AMSCs represent government attempts to blend public and private sector security efforts, private entities have their own individual internal standard operating procedures (SOPs) dealing with security. The private sector is at the forefront of national security due to its physical and economic presence on our borders. The public sector relies on the private sector/private industries to play a key role in not only the planning process, but also the recovery process when disaster strikes. The Maritime Infrastructure Recovery Plan (MIRP) makes note that the private sector plays an important part in planning, operations, and advisory aspects involving port infrastructures.[2] As the private sector continues to grow in the midst of public sector budget constraints, its significance grows, as well. Therein lies the importance of enhancing the private sector's engagement in AMSCs, as well as the strengthening and standardization of private sector SOPs.

Challenges/Issues

[1] U.S. Coast Guard (USCG), U.S. Department of Homeland Security (2015). *Area Maritime Security Committees (AMSC)* Brochure. Retrieved from https://www.uscg.mil/hq/cg5/cg544/docs/AMSC%20Brochure.pdf

[2] U.S. Department of Homeland Security. (2006, April). *The Maritime Infrastructure Recovery Plan.* Retrieved from www.dhs.gov/sites/default/files/publications/HSPD_MIRPPlan_0.pdf

Despite the establishment of dozens of AMSCs throughout the country, attracting private sector members and maintaining consistent and active participation have proven difficult. Since it is a federal program, the pertinent federal law enforcement agencies can be required to attend. Even state, local, or tribal agencies, as part of the public sector, typically are more compelled to attend and participate. The private sector, however, does not have to make AMSC participation a priority, and companies are less likely to participate if doing so is viewed as a hindrance to efficiency and profitability. In 2013, the USCG cited "a decline in support and participation by industry partners in AMSC meetings" for reasons including "increased responsibilities of AMSCs, budget pressure, and the long distances some members must travel for committee meetings."[3] If private sector port security personnel, as potential and desired AMSC members, do not see AMSC participation as a contributor to their respective companies' success, then attendance is unlikely to improve.

Another challenge to private sector integration into AMSCs, specifically, and port security, in general, has been the sharing of sensitive intelligence information. Typically, such information is limited to security and/or intelligence personnel with federal security clearances, or potentially certain members of the non-federal law enforcement community. The private sector cannot be expected to contribute to improving the security environment at our nation's ports if they lack critical information on threats and vulnerabilities that would enable them to do so. As the 9/11 Commission Report noted, the challenge for the intelligence community is finding ways to better support public-private security groups without risking legitimate national secrets.

The aforementioned challenges fall mostly on the shoulders of the public sector, and the private sector also faces its own issues when it comes to incorporating security to the level the

[3] USCG, U.S. Department of Homeland Security. (2013, December 20). *Area Maritime Security Committees: Challenges, Accomplishments, and Best Practices Annual Report.* Retrieved November 5, 2015, from US Coast Guard: http://www.uscg.mil/hq/cg5/cg544/docs/AMSC%20Report%2020DEC13.pdf

government would prefer. The root cause of these issues typically can be traced to a lack of funding and/or material resources, along with a lack of standardization. Most successful private sector firms operating in the maritime port industry have their own security programs, which can incorporate various security measures from uniforms and physical access restrictions to cyber threats and employee health and safety. These internal SOPs can and do vary from one company to another, however, thereby presenting an opportunity for gaps in the overall security of maritime ports.

Actions Taken

As previously discussed, the need for private sector engagement in the realm of maritime port security was one of many shortcomings identified during the detailed scrutiny of U.S. national and homeland security in the wake of the September 11, 2001 attacks. Accordingly, efforts have been made through various initiatives to increase private sector involvement in port security. Some of these efforts are the result of legal requirements, such as Presidential Policy Directive-21[4] regarding critical infrastructure security and Executive Order 13636[5] specifically governing cybersecurity, which "require federal agencies to collaborate with their respective industry sectors" to identify vulnerabilities to critical infrastructure.[6] Some of the actions taken to-date towards increasing private sector engagement are highlighted below.

One of the most significant attempts to bring together members of both the government and private sector with a shared stake in port security was the creation of the AMSC. Run by the U.S. Coast Guard (USCG) within the Department of Homeland Security (DHS), each AMSC is composed of at least seven members, all of whom may be selected from various organizations

[4] The White House Office of the Press Secretary (2013, February12). *Presidential Policy Directive-21: Critical Infrastructure Security and Resilience*. Retrieved from: https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[5] National Archives and Records Administration (2013, February 19). *Executive Order 13636 Improving Critical Infrastructure Cybersecurity*. Retrieved from: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[6] USCG, U.S. Department of Homeland Security. (2013, December 20). *Area Maritime Security Committees: Challenges, Accomplishments, and Best Practices Annual Report.* Retrieved November 5, 2015, from US Coast Guard: http://www.uscg.mil/hq/cg5/cg544/docs/AMSC%20Report%2020DEC13.pdf

and agencies, public and private, with legitimate interest in security operations at the given port. At least seven of these members must have at least five years' experience in the field of maritime/port security operations. AMSCs are responsible for identifying critical port infrastructure and operations; identifying risks; determining mitigation strategies and implementation methods; developing and describing the process to continually evaluate overall port security; and providing advice to, and assisting the Captain of the Port (COTP) – the Coast Guard officer responsible for the port – in developing the AMS Plan.[7]

While AMSCs provide the forum in which the public and private sectors can interact and collaborate on port security, additional measures have been taken to facilitate communication and the flow of sensitive information. In order to minimize the need to sanitize certain security-related intelligence products for dissemination to AMSC members not normally privy to such information, they have the opportunity to be granted a limited scope security clearance through the State, Local, and Industry (SLI) Program. Non-federal AMSC members, whether government or civilian, may request the clearance via the COTP and must undergo the same background investigation process as the federal members in order to obtain the clearance. This willingness to take the necessary steps to share pertinent security information is an important step on the part of the federal government.

Additionally, the Transportation Worker Identification Credential (TWIC), administered federally by the Transportation Security Administration (TSA), conducts security screenings of all employees with port access, to include those of the private sector.[8] With this program the federal government emphasizes the importance of screening all port employees while shouldering some of the workload to do so. The Customs-Trade Partnership Against Terrorism (C-TPAT), administered by U.S. Customs and Border Protection (CBP), is another example of a

[7] USCG, U.S. Department of Homeland Security (2015). *Area Maritime Security Committees (AMSC)* Brochure. Retrieved from https://www.uscg.mil/hq/cg5/cg544/docs/AMSC%20Brochure.pdf

[8] Transportation Security Administration, U.S. Department of Homeland Security (2015). *Transportation Worker Identification Credential (TWIC).* Retrieved from: https://www.tsa.gov/for-industry/twic

government program in which participants from the private sector fulfill certain security requirements in exchange for various benefits in streamlining the customs inspection/clearance process.[9] Private sector entities also can utilize free government resources via the America's Waterway Watch (AWW) program to educate their employees on how/when to report suspicious activity.[10] All of these government programs are available to the private sector, and information regarding their potential benefits to private sector participants can be better disseminated through the forum provided by AMSCs.

While organizations within the private sector may tailor their individual security programs to their specific niche, they do not have to rely upon developing their own processes from scratch. There are frameworks in place to facilitate efficiency and interoperability among legitimate parties to ensure everyone is speaking the same language. These include various U.S. government programs, as well as standards established by the International Organization for Standardization (ISO)[11] and the World Customs Organization (WCO).[12]

Recommendations/Best Practices

Ports are fundamentally vulnerable to terrorist attacks and criminal activity due to their sheer size and the multifarious nature of the many varied port environments that exist throughout the U.S. and the world. AMSCs are vital links among all parties with a stake in U.S. port security and, as such, private sector participation should be encouraged and actively sought by participating government representatives. AMSCs provide an effective and efficient means for regular, open communication and information sharing among the various port security actors from both the public and the private sectors. The committees promote a collaborative

[9] U.S. Customs and Border Protection, U.S. Department of Homeland Security (2015). *Customs and Trade Partnership Against Terrorism (C-TPAT).* Retrieved from: http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism

[10] USCG (2015). *America's Waterway Watch*. Retrieved from: http://americaswaterwaywatch.uscg.mil/What_Else_Should_I_Do.html

[11] International Organization for Standardization (2015). *About Us*. Retrieved from: http://www.iso.org/iso/home.htm

[12] World Customs Organization (2015). *About Us: WCO Goals.* Retrieved from: http://www.wcoomd.org/en/about-us/what-is-the-wco/goals.aspx

environment in which all interested parties contribute to update and improve port security plans and procedures, thereby helping to secure U.S. critical infrastructure in a broader context. Engaging with the AMSCs provides private industry actors with invaluable information from a variety of different perspectives, giving them a comprehensive awareness and working understanding of the complex dynamics of the security issues throughout the port. This sharing of information was the most critical missing component of U.S. security failures that led up to the 9/11 attacks.[13] To enable a cultural shift from 'need to know' to 'need to share', the intelligence community must consider ways to better integrate with private sector partners.[14] AMSCs directly address the issue of interagency communication for the sake of critical infrastructure security and, accordingly, should be treated seriously and promoted aggressively.

At a minimum, the COTP or his/her designee should seek to recruit private sector security officials at a given port to participate actively in the AMSC. If the federal government is serious in its belief in the incalculable value of the private sector when it comes to port security, and if private sector AMSC participation continues to wane, the government could also consider mandating participation for private commercial enterprises that wish to conduct business in a port. The key in selling such a requirement is to emphasize the extensive benefits that accompany AMSC participation, namely access to critical information that facilitates safe and secure operation for all parties in the port, in exchange for relatively little resource expenditure by the private parties involved. Issues such as the time and travel distance required of some private sector AMSC participants have been cited as reasons for a decline in participation. The COTP should take actions to facilitate ease of participation in such cases, such as permitting

---

[13] 9/11 Commission. (2004, July 22). *The 9/11 Commission Report: Final Report of the National Commission on the Terrorist Attacks Upon the United States, Executive Summary.* Retrieved November 8, 2015, from 9/11 Commission: http://www.911commission.gov/report/911Report_Exec.pdf

[14] USCG, U.S. Department of Homeland Security. (2013, December 20). *Area Maritime Security Committees: Challenges, Accomplishments, and Best Practices Annual Report.* Retrieved November 5, 2015, from US Coast Guard: http://www.uscg.mil/hq/cg5/cg544/docs/AMSC%20Report%2020DEC13.pdf

meetings, or even seminar type exercises, via secure video teleconference.[15] Efficient and productive AMSC meetings and exercises are crucial to valuing members' time.

Participation in AMSCs could also increase private sector awareness of other government port security programs that seek to involve the private sector. The federal government should ensure frequent, targeted dissemination of information to the private sector regarding programs such as SLI, TWIC, AWW, C-TPAT, etc. in order to enhance awareness of their availability and utility. AMSCs can provide a perfect avenue through which to ensure such information finds its way to its intended audience. Participation in such programs should, then, be incorporated into private sector internal SOPs. The government should encourage incorporation of such pertinent security practices at a foundational level in order to promote standardization, helping to close security gaps in the global supply chain and ease management of port security as a whole.

Actors within the private sector, in-turn, must make significant efforts to participate in the port security process. Engaging with the AMSC provides the opportunity to regularly weigh in and express concerns from the private sector/industry perspective. In AMSCs, the private sector members are regarded and operate as equal partners, and the information and input on their security concerns assist the USCG in their operations, planning, and production of port security procedures. AMSCs across the nation provide private sector stakeholders a partnering role in informing the decision making process, rather than just lending information or services as requested. Therefore, the private sector should regularly engage with the AMSC and influence the revision of port security procedures and protocols to better represent the private sector perspective.

Private partners in the port industry should also maintain their own robust internal security procedures, consistent both with the needs of individual company along with the public

[15] USCG, U.S. Department of Homeland Security. (2013, December 20). *Area Maritime Security Committees: Challenges, Accomplishments, and Best Practices Annual Report.* Retrieved November 5, 2015, from US Coast Guard: http://www.uscg.mil/hq/cg5/cg544/docs/AMSC%20Report%2020DEC13.pdf

sector's overall goals for infrastructure security. The private sector can do so by investing resources into their own security, while simultaneously making use of the many security programs and free resources made available by the government. Local authorities can also coordinate with the private sector to apply for and tailor federal grant funds to meet the unique needs of their specific port of interest via the Port Security Grant Program.[16] Furthermore, private sector companies involved in port security should develop, write, and update their port facility security plan (FSP) as part of their SOPs in order to mitigate identified risks.

Many port organizations already have internal security procedures that should be universal. Some of these include: uniforms treated as controlled/accountable items; security/access badges, with varying levels of access depending on one's duties; audio/video monitoring and recording; hiring guards or contracting for physical security patrols; and cyber threat analysis. The latter, cyber threats, requires significant attention in today's increasingly digitally dependent world. Maritime ports are no different from most modern industries in their heavy reliance on technology, both on ship and on shore, so cyber risks can be very complex and jeopardize the safety and security of port operations.[17] In the end, private sector port security partners need to make sure security is a fundamental part of their SOPs, as "the development and use of SOPs are an integral part of a successful quality system, as it provides individuals with the information to perform a job properly and facilitates consistency in the quality and integrity of a product or end-result."[18]

---

[16] Federal Emergency Management Agency, U.S. Department of Homeland Security. (2015). *FY2015 Port Security Grant Program*. Retrieved from: http://www.fema.gov/fiscal-year-2015-port-security-grant-program

[17] Thomas, P. (2015, October 8). *Cyber Risks and the Marine Transportation System*. Retrieved November 4, 2015, from www.dhs.gov: http://www.dhs.gov/news/2015/10/08/written-testimony-uscg-house-homeland-security-subcommittee-border-and-maritime

[18] Kenneth, Christopher. (2015). *Port Security Management, Second Edition*. Taylor & Francis Group: Boca Raton, FL. Retrieved from https://books.google.com/books?id=D-jMAwAAQBAJ&pg=PA225&lpg=PA225&dq=private+sector+port+security+standard+operating+procedures&source=bl&ots=KYg1pcRJUb&sig=59ockjmMKV-

AMSCs involve all levels of government and any industry partners to work together and build upon and maintain maritime security. Unity of effort to combat any security threat and cooperating with others to ensure proper security is imperative.[19] Any organization involved in the maritime industry should choose to participate in the AMSCs to enable information dissemination and to take advantage of training opportunities regarding new threats or security procedures. The resources and knowledge of the private sector can be of great value to the U.S. government, and vice versa, as all parties seek to make ports more resilient. Ultimately, communication is the most important practice identified relating to increasing private sector participation in AMSCs and incorporation of enhanced security measures into private organization SOPs. Information needs to be shared in both directions. The government needs to incentivize the programs it already has to make them appealing to companies focused on their bottom line. And private companies with a stake in U.S. port operations need to take responsibility to contribute to and facilitate a collaborative and efficient security environment. All of these actions must occur not only to protect the integrity of the portion of the U.S. commercial supply chain that transits the nation's maritime ports, but to promote U.S. national security.

EtBCjm4cbAFP23PA&hl=en&sa=X&ved=0CB0Q6AEwAGoVChMIrvnd-Yn4yAIVSEGICh0dDAfj#v=onepage&q=standard%20operating%20procedure&f=false

[19] Thomas, P. (2015, October 8). *Cyber Risks and the Marine Transportation System*. Retrieved November 4, 2015, from www.dhs.gov: http://www.dhs.gov/news/2015/10/08/written-testimony-uscg-house-homeland-security-subcommittee-border-and-maritime

“Private Sector Port Security Practices: Best Practices of Selected Asian Ports”

Adam Kyle Mills
Master of Public Affairs/Doctor of Jurisprudence
Expected Graduation: May 2016

Frederick Charles Sadtler
Graduate Certificate in Homeland Security & Emergency Management
Expected Graduation: May 2017

Andrew Robert Smith
Master of Science in Criminal Justice & Public Safety
Expected Graduation: May 2017

Joshua Lynn Welch
Master of Science in Criminal Justice & Public Safety
Expected Graduation: December 2016

Indiana University School of Public and Environmental Affairs
Indiana University – Purdue University Indianapolis

This case study exams selected Asian ports with focus on the history of port development, port management and operation, and advancements in security measures and practices. Recommendations are proposed for improving U.S. security, based on ports studied in the Philippines, Vietnam, Malaysian, and Indonesia. For each port, the Situation, Challenges and Issues, and Current Actions to Mitigate Challenges and Issues are reviewed. The case study concludes with Recommended Improvements for Best Practices.

Philippines – Situation

In the 1970s, before the creation of the Philippine Ports Authority (PPA), there were 591 national and municipal ports plus 200 private ports throughout the Philippines. The need for long-range planning and rationalization of port development became apparent. The Filipino government created the Philippine Ports Authority under Presidential Decree No. 505, with later amendments, which “broadened the scope and functions of the PPA.” In 1978, Presidential Executive Order No. 513 granted police authority to the PPA and created a National Ports Advisory Council to strengthen cooperation between the government and private sector. The PPA is now attached to the Department of Transportation and Communications for policy and

program coordination.[1] The PPA is responsible for management, operations, and finance of all public ports in the Philippines, with the exception of Port Cebu.

Philippines – Challenges and Issues

The International Ship and Port Facility Security (ISPS) Code was implemented by ports under PPA jurisdiction. Per the 2013 PPA Annual Report, the ISPS Code "has been an essential part of the Authority's general security policies designed to establish an international framework involving Governments, Port Authorities, and Shipping and Port Industries to detect security threats and undertake preventive measures against security incidents affecting ships or port facilities used in international trade." Specific to the ISPS Code, a study was conducted to discover compliance of major Filipino ports to requirements of the Code and level of knowledge and awareness of port personnel in the proper implementation, compliance, and evaluation of the Code. The safety and security of these ports, and others worldwide, largely depends on management of the port authorities in conjunction with the ISPS Code. The PPA has since taken steps to familiarize all personnel and key stakeholders on the concepts and principles of maritime and port security.

Philippines – Current Actions to Mitigate Challenges and Issues

In 2004, Port Management Officers in the Philippines submitted revised Port Facility Security Plans in accordance with the ISPS Code. Since then, the study has determined all Filipino ports are ISPS Code compliant. In fact, "the port authorities are strictly implementing the provisions and are also taking all necessary precautions in order not to repeat the experiences

[1] Philippine Ports Authority (2015). *About Us – History*. Philippine Ports Authority. Retrieved from http://www.ppa.com.ph/

of September 11, 2001."[2] The work being undertaken by Filipino ports helps ensure global security, with undoubted impact upon the U.S. Additionally, the PPA operates a Vessel Traffic Management System (VTMS), whose Control Center is a "state-of-the-art vessel monitoring facility managed and operated by PPA on a 24/7 basis. The operation of VTMS focuses on giving round-the-clock assistance as well as relaying information to pertinent government agencies incidents of vessel distress, accidents, piracy, and others for appropriate action."[3] Since implementation, the VTMS has served as both an effective navigational tracking tool and has increased security measures at the three major ports where installed.

The Philippine government partners with the U.S. to improve port security. For example, in 2011, the U.S. government contributed over $26 million for upgrading of radiation detection capabilities in Asian Terminal Incorporated's South Harbor and the International Container Terminal Services, Inc.'s Manila International Container Terminal. The governments hope the upgrades will prevent movement of radioactive or nuclear material through Philippine ports, and therefore prevent terrorist activity involving such materials.[4]

Vietnam – Situation Vietnam is quickly becoming a global leader in exporting. In 2014, Vietnamese container ports experienced the largest growth rate in the world[5]. Vietnam has a total

[2] Weintrit, A. and Neumann, T. (2013). Marine Navigation and Safety of Sea Transportation: Maritime Transport and Shipping. Pages 133-137. CRC Press. Retrieved from https://books.google.com/books?id=Ax8l-UkmsEkC&pg=PA136&lpg=PA136&dq=top+three+ports+in+the+philippines&source=bl&ots=Disx2egyNM&sig=z1_GaEVZlz_XPsgnRe8XKRlJP0A&hl=en&sa=X&ved=0CDgQ6AEwBWoVChMIztyT6MGJyQIVRNgeCh1O2wIn#v=onepage&q=top%20three%20ports%20in%20the%20philippines&f=false.

[3] Monitoring and Evaluation Division, Strategic Planning Department. (2014). *2013 Annual Report*. Philippines Ports Authority. Retrieved from http://www.ppa.com.ph/AnnualReport/Final%20PPA%20AR%202013.pdf

[4] Embassy of The United States. (2011, September 13). Philippines and U.S. Commission Megaports System to Increase Security at the Port of Manila. Retrieved from http://manila.usembassy.gov/megaports.html

[5] Too Many Vietnam Seaports Spoiling Terminal Business, Bloomberg News (March 18,2014) Retrieved From: http://www.bloomberg.com/news/articles/2014-03-14/too-many-vietnam-seaports-spoiling-terminal-business

of 114 seaports, with 14 key to economic development due to their size[6]. The remaining 100 are small and have poor supporting services and facilities. The three largest ports in Vietnam include the Saigon port, the Hai Phong port, and the Da Nang port.[7]

Vietnam – Challenges and Issues

While Vietnam has robust export numbers, the fact that many nearby nations have developed better seaports and shipping options cannot be overlooked. Most of the challenges faced by Vietnam's seaports can be traced back to a lack of progress in building and growing their sea ports. Simply put, most of Vietnam's neighbors have had more time to grow their sea port and exporting industries. One of the major challenges faced in Vietnam is overall connectivity. Sea ports must have reliable transportation infrastructure; highways, railways and connecting roads in between. Vietnam also lacks an overall sea port plan and some of their sea ports are not developed and planned properly for future cargo. Vietnam has a tax and fee collection system that makes it more difficult for cargo freighters to operate. Another key issue faced by seaports in Vietnam is the decentralized nature of government in the country. The provinces have a great deal of political power according Nguyen Xuan Thanh a Harvard's Kennedy School of government representative in Vietnam.[8]

Vietnam – Current Actions to Mitigate Challenges and Issues

Vietnam is a key location, with nearly 2,000 miles of coast in the Gulf of Tonkin and the South China Sea. The nation is actively working to improve their sea ports, and Vietnam does

---

[6] Runckel, C. W. (2006). Ports in Vietnam stunting amid economic development. Retrieved from Business in Asia: http://www.business-in-asia.com/ports_in_vietnam.html

[7] Runckel, C. (n.d.). Seaports in Vietnam. Retrieved November 10, 2015, from http://www.business-in-asia.com/ports_in_vietnam.html

[8] Laursen, W. (2015, May 20). Vietnamese Container Ports Top 2014 Growth. Retrieved from The Marine Executive : http://www.maritime-executive.com/article/vietnamese-container-ports-top-2014-growth

have advantages in the region, including an abundance of low wage workforces and people willing to work. These advantages will continue to drive investments. Vietnam also finds itself in a pitched competition with nearby nations. The hotly contested Spratly islands show the importance of this region's exporting industry. As this importance is realized by the Vietnamese government, there has been a concerted effort to expand the nation's port capabilities. In a 2014 article in the Bloomberg News there was concern by the director of the CIA Mep international terminal near Ho Chi Minh City that the government was pushing to increase the number of seaports in the country. The fear is that an over saturation of ports would lead to corruption.[9]

The Vietnam government has been increasingly active and forthright in its plans to increase, expand, and improve their port systems in the country. The government has set forth admirable goals and intricate plans for how to achieve these goals. The process for which these goals and plans are carried out in Vietnam are based on decentralization policies which distribute the power, influence, roles and responsibilities throughout the Vietnamese government. As such, in the case of port initiatives and decision making the process initially begins with the highest level of the Vietnam Government, but then, passed down to Provinces for implementation. Districts or commune level government officials actually carry out implementing the initiatives in their areas that are affected by them. Therefore, the decentralized government/policies involves all levels of implementation.[10]

Malaysia – Situation Malaysia's Port Klang, the country's largest port and gateway to the capital of Kuala Lumpur, consistently ranks among the world's busiest maritime ports, with

[9] Too Many Vietnam Seaports Spoiling Terminal Business, Bloomberg News (March 18,2014) Retrieved From: http://www.bloomberg.com/news/articles/2014-03-14/too-many-vietnam-seaports-spoiling-terminal-business

[10] de Wit, J.W, Viet Sang, L, Van Chien, L, Thu Hien, L, Viet Hung, H, Thi Anh Tuyet, D, … Thi Thanh Tam, M. (2012).Assessing decentralised policy implementation in Vietnam : The case of land recovery and resettlement in the Vung Ang Economic Zone (No. 546). ISS Working Paper Series / General Series (Vol. 546, pp. 1–55). Erasmus University Rotterdam. Retrieved from http://hdl.handle.net/1765/32910

throughput of nearly 11 million TEU in 2014.[11] The three ports that comprise Port Klang – Northport, Southport, and Westport are administered by private corporate entities, yet they are responsible to the regulation of the local Port Klang Authority (PKA). The PKA, subsequently, reports to the national level Royal Malaysian Customs Department.[12]

Malaysia – Challenges and Issues

The narrow, 550-mile waterway straddling Indonesia, Malaysia and Singapore is a key commercial maritime route carrying a third of the world's trade and half of the world's oil supply. The port serves as origin, destination, and transit point for passenger, shipping, and military vessels from all over the world and, therefore, also represents a significant target for would-be criminal or terrorist activity. As such, security of the supply chain at Port Klang is of particular interest to the United States. Some of the security practices employed at Port Klang also can be seen at many U.S. ports, or should be implemented if not currently in place.

Malaysia – Current Actions to Mitigate Challenges and Issues

Port Klang was an early partner with U.S. Customs and Border Protection in its Container Security Initiative implemented in the wake of the 9/11. CBP deploys personnel to ports around the world to partner with host nation customs officials in an effort "to target and prescreen containers and to develop additional investigative leads related to the terrorist threat to cargo destined to the United States."[13] Port Klang subscribes to recommendations from the World Customs Organization on how major ports can facilitate security of the global supply chain.[14] During a summit in 2005, WCO personnel highlighted Port Klang's extensive coordination among all parties with interest in port operations, from both the government and private sector,

[11] Port Klang Authority (2015, November 11). Retrieved from: http://www.pka.gov.my/
[12] Royal Malaysian Customs Department (2015, November 11). Retrieved from: http://www.customs.gov.my/en
[13] U.S. Customs and Border Protection (2015, November 11). *Container Security Initiative*. Retrieved from: http://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief
[14] World Customs Organization (2015, November 11). *Security Programme*. Retrieved from: http://www.wcoomd.org/en/topics/enforcement-and-compliance/~/link.aspx?_id=CC42F6A5A9B340109FF1ABB96BE5EC41&_z=z

as critical to the security effort. They also noted the importance of effective human resource development, focusing not only on hiring the right employees to bring in more revenue, but also "to embrace a wider range of functions including protection of the community, economic development, and national security."[15] Given its location along strategic trade routes and proximity to multiple Asian powers, Malaysia occasionally coordinates military exercises and operations with other nations in the region.[16] These efforts deal extensively with maritime piracy issues, as many vessels that transit through Port Klang have been targets of pirates.[17] Westport has been recognized as both safe and secure on an international level. The adoption of smart card and EDI technology has been a huge asset in security access measures to the port. This has reduced lost containers and container theft from the port provided cargo owners extra assurance of safety.[18] The Northport section reports utilizing 24/7 video surveillance of all entry and exit points, roving physical security, and a 24/7 on-call emergency response team. The presence of the Port Klang Free Zone, essentially a duty free zone for shipping and manufacturing that is physically located at the port, yet technically outside of Malaysia to provide certain economic incentives for participants, should require even more deliberate scrutiny to ensure security measures are not circumvented.[19] Razali and Dahalan[20] conclude that implementation of the ISPS Code in the federal Malaysian ports has had positive implications for port and ship security and

---

[15] World Customs Organization (2005, March 31). *WCO Initiatives Enhance Security and Facilitation Measures at Port Klang in Malaysia*. Retrieved from: http://www.wcoomd.org/en/media/newsroom/2005/april/wco-initiatives-enhance-security-and-facilitation-measures-at-port-klang-in-malaysia.aspx

[16] Want China Times (2015, September 17). *China and Malaysia Hold Naval Exercise in Strait of Malacca*. Retrieved from: http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20150917000176&cid=1101&MainCatID=11

[17] Rider, David. (2015, February 17). *Maritime Security Review*. "ReCAAP Reports on Hijacking, IED." Retrieved from: http://www.marsecreview.com/2015/02/recaap-reports-on-hijacking-ied/

[18] *Smart card & EDI*. (n.d.). Retrieved November 11, 2015, from Our Port: http://www.westportsmalaysia.com/Technology-@-Smart_Card_-%E2%97%98-_EDI.aspx

[19] Port Klang Free Zone (2015, November 11). *PKFZ Profile*. Retrieved from www.pkfz.com

[20] Razali, N.H., Dahalan, W.S. (2012). The ISPS Code and It's Implementation in Malaysia. *Arena Hukam*, 6, 42-47.

has reduced their vulnerability to terrorist attacks. Improvements have been realized in the following areas; the level of physical and procedural security of ships and port facilities has been enhanced, good relationships have been developed between the Ministry of Transport and Security Officers, which improves cooperation in detecting and deterring security threats, and the training and heightened awareness of security has promoted good relations between shipping lines and port operations.

Indonesia – Situation

Indonesia is a large spread out region, made up of over 17,000 islands. Like many of the islands, the respective ports vary greatly in size with approximately 154 active ports. As such, Indonesia is dependent on ports for the majority of its domestic transportation and international trade.[21] A seaport may be hundreds of miles closer than other transportation options. In 2009, Indonesia moved 968 million tons of cargo through its ports.

The majority of ports are managed by the Indonesia Port Corporation, a state-owned government enterprise.[22] Indonesia has four state owned port operators, which are known as Pelindos I, II, III, and IV.[23] The state-owned enterprises history dates back to the 1960's when the government established Perusahaan Negara Pelabuhan, eight state-owned enterprises. Throughout the years there have been many changes to how ports are controlled. From the 60's trough the 90's, Perusahaan Umum (Perum) was established to go from individual companies to a single public corporation.

Indonesia – Challenges and Issues

[21] OECD Reviews of Regulatory Reform: Indonesia. (2012, September 1). Retrieved December 2, 2015, from http://www.oecd.org/indonesia/Chap 5 - Ports Rail and Shipping.pdf
[22] Pelabuhan Indonesia II (SOE). (n.d.). Retrieved December 2, 2015, from http://www.indonesia-investments.com/business/indonesian-companies/pelabuhan-indonesia-ii/item337
[23] Dodd, C. (2015, February 28). Indonesia launches massive port expansion. Retrieved November 12, 2015, from http://www.financeasia.com/News/394905,Indonesia-launches-massive-port-expansion.aspx

Specifically, Pelindo II operates twelve commercialized ports in ten provinces. The busiest port in Indonesia, Port Tanjung Priok, located in a sub-district of Jakarta, handled 102.5 million tons of cargo in 2010.[24] Although it handles over 2/3 of Indonesia's entire world trade, the container traffic here is expected to grow by over 160% this year alone.[25] The activity that this port usually encounters is cargo vessels and tankers. Due to the high amount of traffic, the dwell time is longer. This not only costs the businesses because the products are not getting shipped, but also costs the consumer due to the high demand for goods that are delayed.

Indonesia – Current Actions to Mitigate Challenges and Issues

The Indonesian government is increasing funding to upgrade port infrastructure. The Tanjung Priok Port is adding three new terminals as an extension called the Kalibaru Port to cut transport and handling time in half.[26] This will increase overall productivity of the port. While Pelindos II is adding and expanding, Pelindos I for example, plans to modernize and expand ports over the next five years.

The US Coast Guard press release dated January 02, 2013 reviews progress Indonesia has made in port security. This was release was after 34 Indonesian ports had been placed on the Port advisory list amidst repeated security concerns for a three period in 2005-2008.[27] The US Coast Guard, as part of the International Ship and Port Facility Security (ISPS), found vast improvement following inspections conducted after Indonesia was placed on the advisory list.

---

[24] WPS - Home Page. (n.d.). Retrieved November 11, 2015, from http://www.worldportsource.com/
[25] Moving Cargo Faster in Indonesia's Main Sea Port. (2014, February 19). Retrieved December 2, 2015, from http://www.worldbank.org/en/news/feature/2014/02/19/moving-cargo-faster-in-indonesia-main-sea-port
[26] Dodd, C. (2015, February 28). Indonesia launches massive port expansion. Retrieved November 12, 2015, from http://www.financeasia.com/News/394905,Indonesia-launches-massive-port-expansion.aspx
[27] USCG, News Release. *Indonesia Improves Port Security wit Coast Guard Assistance*. (January 02, 2013), 14t District Hawaii & Pacific Public Affairs. Retrieved From: http://www.uscgnews.com/go/doc/4007/1671215/Indonesia-improves-port-security-with-Coast-Guard-assistance#

By 2011, all Indonesian ports were removed from further in depth inspection as antiterrorism measures had greatly improved.

Recommended Improvements for Best Practices:

Based on our review of selected Asian ports, two types of port security initiatives standout as key to improving U.S. port security; implementation of the ISPS Code abroad and U.S. partnerships which target specific port security technology and programs. Continued implementation and surveillance of the ISPS Code requirements at ports abroad was cited in three of the four countries studied as an essential factor in raising the overall port security level. The ISPS Code requirements apply to all parties involved in port operations; port authorities, governmental agencies, security teams, and private sector terminal operators and shippers.

U.S. partnership examples were cited as key security initiatives for ports in the Philippines and Malaysia. Partnerships in the Philippines have helped fund specific technology to detect radioactive or nuclear materials and therefore prevent terrorist from using these as weapons of mass destruction. Malaysia partners with the U.S. Customs and Border Patrol in the implementation of the Container Security Initiative to target and pre-screen containers bound for the U.S. This initiative works through local port authorities, agencies and terminal operators to prevent suspect containers from being shipped to U.S. ports. Continuing to fund program and technology partnerships with foreign ports will have significant benefits to U.S. port security.