

UNITED STATES SEAPORT SECURITY:
PROTECTION AGAINST A NUCLEAR DEVICE ATTACK
DELIVERED IN A SHIPPING CARGO CONTAINER

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
Homeland Security Studies

by

ROMMEL P. AQUINO, MAJ, USAR
B.S., University of Illinois at Chicago, Chicago, IL, 2001
M.A., Webster University, St. Louis, MO, 2010

Fort Leavenworth, Kansas
2014-01

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 13-06-2014		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) AUG 2013 – JUN 2014	
4. TITLE AND SUBTITLE United States Seaport Security: Protection Against a Nuclear Device Attack Delivered in a Shipping Cargo Container				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Aquino, Rommel P., Major, U.S. Army Reserves				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301				8. PERFORMING ORG REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for Public Release; Distribution is Unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The aftermath of the 11 September 2001 terrorist attacks on the United States refocused the nation's attention on homeland security. The safety and security of the United States rely not only on the nation's ability to protect itself from a terrorist attack, but also to secure its economy through international trade. The primary question of this thesis is: What are the current standard procedures for inbound cargo inspections in U.S. seaports, and which actions have been taken to meet the 2007 congressional directive for 100-percent inspection of weapons-grade nuclear and radioactive substances prior to departure from foreign seaports? Three ports—Long Beach, Miami-Dade, and Houston—are provided for case analysis. Each port is analyzed for the security plan in place, the roles and coordination among its security partners, the application of the security plan and current technology, and the amount of federal funding awarded to each port and how much is apportioned toward enhancing port security. The point of origin from which the cargo containers come still has not met the congressional mandate of 100-percent scanning of radiological and nuclear material. This vulnerability will need federal attention.					
15. SUBJECT TERMS Homeland Security, Seaport Protection, Federal Funding, Maritime Security Programs, Terrorist Attack, Response and Recovery, Port of Long Beach, Port of Houston, Port of Miami-Dade, Terrorist Attack, Cargo Container					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. PHONE NUMBER (include area code)
(U)	(U)	(U)	(U)	99	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Rommel P. Aquino

Thesis Title: United States Seaport Security: Protection Against a Nuclear Device
Attack Delivered in a Shipping Cargo Container

Approved by:

_____, Thesis Committee Chair
COL Dawn D. DeVine, MSA, MSS.

_____, Member
O. Shawn Cupp, Ph.D.

_____, Member
Don A. Myer, M.SSM.

Accepted this 13th day of June 2014 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

UNITED STATES SEAPORT SECURITY: PROTECTION AGAINST A NUCLEAR DEVICE ATTACK DELIVERED IN A SHIPPING CARGO CONTAINER, by MAJ Rommel P. Aquino, 99 pages.

The aftermath of the 11 September 2001 terrorist attacks on the United States refocused the nation's attention on homeland security. The safety and security of the United States rely not only on the nation's ability to protect itself from a terrorist attack, but also to secure its economy through international trade. The primary question of this thesis is: What are the current standard procedures for inbound cargo inspections in U.S. seaports, and which actions have been taken to meet the 2007 congressional directive for 100-percent inspection of weapons-grade nuclear and radioactive substances prior to departure from foreign seaports? Three ports—Long Beach, Miami-Dade, and Houston—are provided for case analysis. Each port is analyzed for the security plan in place, the roles and coordination among its security partners, the application of the security plan and current technology, and the amount of federal funding awarded to each port and how much is apportioned toward enhancing port security. The point of origin from which the cargo containers come still has not met the congressional mandate of 100-percent scanning of radiological and nuclear material. This vulnerability will need federal attention.

ACKNOWLEDGMENTS

I would like to express my appreciation and thanks to COL Dawn Devine, Dr. O. Shawn Cupp, and Mr. Don Myers for serving as my committee members and guiding me throughout this past year. Dr. Cupp, you have provided tremendous support in my goal to complete this thesis. I would like to thank you for encouraging my research and for allowing me to grow as a research student. Your advice on both research and my career has been priceless. I also want to thank you for letting my comprehensive oral exam and defense be an enjoyable moment, and for your comments and suggestions. I would especially like to thank Carolyn Allard, my editor, whose recommendations, guidance, and expertise kept me focused on the importance of the research. Without her assistance, I would not have completed this research within the required time frame.

A special thanks to my family. Knowing that my family supported my efforts and goals and was always there to help my wife and kids in their times of need cannot be conveyed in words. Lastly, I would like to express appreciation to my beloved wife of eleven years, Amy, who has kept the family together while I was away from home this past year and who has always supported my career, especially in the moments when I was in need of guidance on which path to take.

TABLE OF CONTENTS

	Page
MASTER OF MILITARY ART AND SCIENCE THESIS APPROVAL PAGE	iii
ABSTRACT.....	iv
ACKNOWLEDGMENTS	v
TABLE OF CONTENTS.....	vi
ACRONYMS.....	ix
ILLUSTRATIONS	x
TABLES	xi
CHAPTER 1 INTRODUCTION	1
Problem Identified	3
Research Question	4
Secondary Questions.....	5
Assumptions.....	5
Key Terms.....	6
Limitations and Delimitations	8
Significance of Study.....	9
Conclusion	10
CHAPTER 2 LITERATURE REVIEW	15
Existing Publications	16
National Strategies and Plans	18
Key Maritime Acts.....	20
Private Sector Think Tanks and Reports	23
Challenges.....	24
Failure to Achieve Directive.....	25
Conclusion	26
CHAPTER 3 RESEARCH METHODOLOGY	29
Background.....	30
Evaluation Criteria.....	30
Seaport Security Plans	31
Application of Guidelines.....	33
Federal Funding	33

Conclusion	34
CHAPTER 4 ANALYSIS	35
Primary Research Question	35
Secondary Research Questions	36
Federal Government Responsibilities	36
State Government Responsibilities	41
Local Government Responsibilities	41
Private Sector Responsibilities	42
Providing and Monitoring Oversight	42
Current Regulations, Policies, and Programs	43
33 Code of Federal Regulation Subchapter H – Maritime Security	43
33 U.S. Code § 1226 – Port, Harbor, and Coastal Facility Security	43
MTSA 2002	43
Customs-Trade Partnership Against Terrorism	44
Container Security Initiative	44
Operation Safe Commerce	45
Maritime Administration	45
Megaports Initiative	46
Federal Grant Programs	47
Technology Currently in Place	47
Transportation Worker Identification Credential Program	48
Radiation Portal Monitors	49
Vehicle and Cargo Inspection System	49
Radio Frequency Identification Devices	50
Anti-Tamper Seals	50
Case Study of Houston, Long Beach, and Miami-Dade Seaports	50
Port of Houston Authority	51
Seaport Security Plans and Interagency Coordination	52
Application of Plans and Technology	53
Federal Funding	55
Port of Long Beach	56
Seaport Security Plans and Inter-Agency Coordination	57
Application of Plans and Technology	58
Federal Funding	60
Port of Miami-Dade	60
Seaport Security Plans and Interagency Coordination	61
Application of Plans and Technology	63
Federal Funding	64
Research Evaluation Criteria Chart	64
Conclusion	67
CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS	71
Primary Research Question	71

Secondary Research Questions	72
Overview of Summary of Research.....	74
Case Analysis.....	75
Security Plans.....	75
Current Protective Measures.....	75
Funding	76
Meaning of Findings.....	77
Recommendations.....	79
Funding Allocations.....	79
Department of Defense Assistance	80
Exercise and Training	80
Research and Development.....	81
Global Partnerships	81
Conclusions.....	81
 BIBLIOGRAPHY	 84

ACRONYMS

CBP	U.S. Customs and Border Protection
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FSP	Facility Security Plan
MTSA	Maritime Transportation Security Act
PHA	Port of Houston Authority
PLB	Port of Long Beach
PSGP	Port Security Grant Program
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
USCG	United States Coast Guard
WMD	Weapon of Mass Destruction

ILLUSTRATIONS

	Page
Figure 1. Department of Homeland Security Communication Flow Chart	21
Figure 2. U.S.-Bound Cargo Flow Chart.....	23
Figure 3. Strategic Framework for Securing America’s Borders at Ports of Entry	39
Figure 4. Partnership Relationship Diagram at the Ports	40

TABLES

	Page
Table 1. Blank Case Study Comparison Chart of the Ports of Long Beach, Houston, and Miami-Dade.....	32
Table 2. Case Study Comparison Chart of the Ports of Long Beach, Houston, and Miami-Dade	65

CHAPTER 1

INTRODUCTION

In October 2001, only weeks after the 9/11 attacks on the United States, Italian authorities discovered an Egyptian man suspected to be a member of the Al-Qaeda terrorist network hiding in a shipping container heading to Halifax, Nova Scotia. The container was fully equipped with a bed, toilet, and internal power source to operate heaters and other electronic devices. In addition, the man had possession of a satellite phone, laptop, airline mechanic's certificate, and security passes for airports in Egypt, Thailand, and Canada. The following year, in March 2002, the Norwegian intelligence agency reported that it had identified up to twenty-three merchant ships that were linked to Al-Qaeda and owned by Osama bin Laden and used to transport explosive devices that destroyed the embassies in Kenya and Tanzania in 1998, resulting in the deaths of 234 people, including twelve Americans.

A few months later, in May 2002, U.S.-born and Muslim convert Jose Padilla was arrested in Chicago for plotting to set off a radioactive dirty bomb, and on 29 June Moldavian undercover security agents posing as a North African buyer arrested six men trying to sell stolen uranium. The men were in possession of two kilograms of uranium-235, low-enriched uranium that cannot be used in a nuclear weapon and that is in need of further processing to develop into highly enriched uranium. However, in March 2010, two men were apprehended in Georgia trying to sell eighteen grams of highly enriched uranium, which were weapons grade. Although a minimum of twenty-five grams is needed to create a dirty bomb, a terrorist organization can easily attain more highly enriched uranium and piece together the nuclear material. More recently, in December

2013, Mexican law enforcement reclaimed a stolen truck transporting a highly radioactive isotope, cobalt-60, from a hospital. Although the material is primarily intended for medical treatments and cannot be utilized in a conventional nuclear weapon, it could be added to the materials needed to produce a dirty bomb, having the ability to spread radioactive material over a wide area.¹ These are only a few of the terrorist events that have occurred in the past twelve years and should serve as a warning to the United States for the potential of a nuclear attack on its soil, especially through its seaports.

Although not a terrorist attack, the catastrophic event in Texas City, Texas, on 16–17 April 1947 serves as a reminder of the magnitude of destruction that can result from a large explosion occurring in a seaport. Two ships, SS *Grandcamp* and SS *High Flyer*, both carrying ammonium nitrate, exploded due to an initial fire discovered at the pier warehouse. Fragments from the blast were sent as far as Galveston ten miles away. Approximately 1,000 residence and business buildings were either destroyed or sustained major structural damage, including 1,100 vehicles in the dock parking lot and throughout the city. Nearly 600 people died and 2,000 suffered injuries from flying debris. The estimated cost of the damage was \$35 to \$40 million (much more in today's dollars) and the rebuilding period would take approximately two years. This event not only crippled Texas City's economy but also its way of life as nearly everyone was affected by this tragedy.

More than two-thirds of the world is covered by seawater. Greater than 80 percent of the world trade travels through these maritime routes, and 90 percent of trades are shipped via cargo container. The world's economy is dependent and thrives on the ocean, which allows countries to participate in the global marketplace. Almost 2 billion tons of

cargo in 21 million containers passes through U.S. seaports annually, amounting to nearly \$800 billion worth of domestic and international goods.² U.S. seaports facilitate 95 percent of incoming cargo through 361 ports and are nearly 90 percent crucial to the country's economic strength.³

Terrorist organizations intent on destroying the United States have indicated the desire to acquire and utilize weapons of mass destruction (WMD). The increasing ease of access to new technology and attainment of a delivery platform is a direct threat to U.S. commercial seaports. America's way of life is dependent on the continuous operation of its seaports. A WMD attack on a major commercial seaport can have a catastrophic effect on the economy, population, and critical infrastructure. Distribution and supply lines from the west coast to the east coast would be disrupted, along with America's international partners' ability to conduct trade while recovering from the contaminated area. It is important that the United States focus its attention on the vulnerabilities of its seaports and develop a more effective procedure than what is currently in place to address and prevent a terrorist attack.

Problem Identified

The 9/11 Al-Qaeda attack on the United States prompted the Department of Homeland Security (DHS) to increase airport security measures by tightening screening procedures and improving technology. Established a few months after 9/11, the Transportation Security Administration (TSA) has been in existence for more than twelve years. This organization has nearly 50,000 screeners working at more than 450 airports nationwide, screening a daily average of nearly 1.8 million passengers through its checkpoints.⁴ The failed bombing in 2002 involving Richard Reid (the "shoe bomber")

and the 2009 attempt on Christmas Day involving Umar Farouk Abdulmutallab (the “underwear bomber”) led to the installation of full-body scanners in nearly all major airports across the United States, along with enhanced pat-downs and shoe screenings. However, U.S. seaport security did not receive the same level of attention and progressive improvement as airports did.

Experts in the field of port security believe the next terrorist attack will enter the United States by sea and potentially strike with a WMD.⁵ Although America’s highest priority is preventing terrorists from acquiring a nuclear device, an equal or greater emphasis should be placed on port security. Terrorist organizations driven to destroy the United States physically, economically, and psychologically will continue to exploit vulnerabilities in its security system. There are approximately six million cargo containers arriving in the United States annually (26,000 a day) from all over the world,⁶ and fewer than 5 percent are physically inspected by U.S. Customs and Border Protection (CBP). Due to the risk of a terror strike that uses as its delivery platform an inbound cargo container with a nuclear device (dirty bomb) inside, it is important that DHS institute tighter security protocols and use advance screening systems in U.S. seaports.

Research Question

The thesis question concerns the current security protocols and standard operating procedures of U.S. seaports’ handling of cargo containers. This question will focus on the changes and improvements made to seaport security after the signing of the Maritime Transportation Security Act (MTSA) of 2002 and compared to the post-9/11 response and the procedures followed by DHS. The thesis question is: What are the current standard procedures for inbound cargo inspections in U.S. seaports, and which actions

have been taken to meet the 2007 congressional directive for 100-percent inspection of weapons-grade nuclear and radioactive substances prior to departure from foreign seaports?

Secondary Questions

The following are the subordinate questions to this thesis.

1. If standards have been improved since the MTSA 2002, will they detect and prevent a nuclear dirty bomb device from reaching a major seaport?
2. What current technology is available to screen a higher percentage of cargo containers bound for the United States?
3. Is the United States—specifically DHS—prepared for future terrorist attacks originating from inbound cargo containers?
4. Is it feasible to conduct 100-percent inspection of all U.S.-bound cargo containers?

In addition, current seaport security issues and policies from all federal government agencies must be identified as well as their roles in securing U.S. seaports. This includes not only DHS and its subordinate agencies, but also the Federal Bureau of Investigation, the Central Intelligence Agency, the National Security Agency, and other intelligence agencies.

Assumptions

Based on the historical activities of Al-Qaeda and other terrorist organizations post-9/11, they will continue to plan and execute future attacks on the United States. The improved and tightened security in U.S. airport systems has hindered their ability to

utilize airplanes as avenues of attack. However, U.S. seaport security remains vulnerable for exploitation, specifically inbound cargo containers. The first assumption is that terrorists are continuously seeking ways to attack through the use of U.S.-bound cargo containers. The second assumption is that terrorists continuously strive to attain a nuclear device or radioactive substance that can be transported in an inbound cargo container. The final assumption is that, due to the inevitable budget cuts and the limited manpower of DHS and other federal agencies, the enemy continues to probe and identify vulnerable U.S. seaports that play a major role in its economic system.

Key Terms

The following identify and define the terms presented in this thesis and indicate the manner in which they will be used within context of this research.

Al-Qaeda (translation: The Base). A militant Islamist terrorist organization founded by Osama bin Laden in Peshawar, Pakistan. Its origins can be traced back to the Soviet War in Afghanistan. Al-Qaeda has attacked civilian and military targets in various countries, including the 11 September 2001 attacks, 1998 U.S. Embassy bombings, USS *Cole* bombings, and 2002 Bali bombings, as well as the kidnappings of western citizens. Techniques employed include suicide attacks and simultaneous bombings of different targets. Al-Qaeda envisions a break from all foreign influence in all Muslim countries and a creation of a new world Islamic order.⁷

Department of Homeland Security. A department of the United States government that was created in response to the 11 September 2001 attacks. Its main responsibility is to protect the United States from terrorism and other hazards.⁸

Dirty bomb. A radiological weapon that combines radioactive material with conventional explosives in order to contaminate an area with the explosion, denying use by civilians.⁹

Domestic Nuclear Detection Office. Responsible for acquiring and supporting the deployment of radiation detection equipment, including Radiation Portal Monitors, at domestic seaports to support the scanning of cargo containers before they enter U.S. commerce.¹⁰

Federal Emergency Management Agency. Responsible for administering grants to improve security of the nation's highest risk port areas.¹¹

Maritime Transportation Security Act of 2002. A law constituted in 2002 designed to protect ports and waterways from terrorist attacks. It requires vessel and port facilities to conduct vulnerability assessments and develop security plans that may include passenger, vehicle, and baggage screening procedures; security patrols; establishing restricted areas; personnel identification procedures; access control measures; and installation surveillance equipment.¹²

National Security Strategy. A document that is prepared periodically and reviewed by the executive branch of the United States government in order for Congress to identify the country's key national security concerns and how the administration will deal with them.¹³

9/11. Attacks coordinated and carried out by the Islamic terrorist group Al-Qaeda on the United States in the New York City and Washington, DC, metropolitan areas on 11 September 2001, killing almost 3,000 people.¹⁴

Osama bin Laden. Islamist militant leader and founder of Al-Qaeda who planned the 11 September 2001 attack on the United States and the U.S. embassy bombings. Killed during a raid by U.S. Special Operations Forces in 2011.¹⁵

Seaport. A town or city with a harbor for seagoing ships, primarily cargo ships carrying containers.¹⁶

Transportation Security Administration. Responsible for managing the Transportation Worker Identification Credential program and designed to control the access of maritime workers to regulated maritime facilities in the United States.¹⁷

United States Coast Guard. Responsible for the safety and security of U.S. maritime interests and leading homeland security efforts in the maritime domain.¹⁸

U.S. Customs and Border Protection. Responsible for the screening of incoming vessels and their crew and maritime cargo for the presence of contraband, such as weapons of mass destruction, illegal drugs, and explosives, while facilitating the flow of trade and passengers.¹⁹

Limitations and Delimitations

America's maritime system has more than 350 sea- and river ports and more than 1,000 harbor channels along thousands of miles of coastline in the continental United States. This research is limited to open source and unclassified documents and materials, primarily federal government documentation from DHS to include Presidential and Congressional directives concerning maritime and port security initiatives. The source dates reflect the time frame of January 2002 through January 2014. In order to support the thesis, it is necessary to thoroughly review documents relating to the initial maritime response post-9/11 and the progress, or lack thereof, from the current time frame. The

emphasis is on nuclear and radiological attacks and the technology used to combat them. The delivery platform for this research is cargo shipping containers, with a specific focus on coastline seaports located in the Pacific Ocean, Atlantic Ocean, and Gulf of Mexico. Inner coastal ports, river terminals, and Great Lakes shipping ports will not be considered. The research on this subject is primarily limited to the U.S. seaport security procedures post-9/11 and will not compare international partners' seaport security protocols. However, some comparisons of pre-9/11 security procedures will be examined in order to show changes that were made prior to the MTSA 2002. This research study will focus specifically on cargo or shipping containers having the ability to hide a nuclear dirty bomb device and serve as a delivery platform for a major attack on a U.S. seaport.

Significance of Study

The United States receives thousands of cargo containers daily from around the world through its seaports, some possibly containing illegal materials or worse—items that can directly affect national security. This research is significant in relation to U.S. homeland security. In the MTSA 2002, Congress noted the following findings concerning U.S. seaport security measures (a total of fifteen findings were identified in the MTSA 2002; listed here are the findings that relate to this research paper).²⁰

1. The top fifty ports in the United States account for about 90 percent of all cargo tonnage and twenty-five ports account for 98 percent of all container shipments.
2. Ports are major operation areas for federal crime, including drug trafficking, cargo theft, and smuggling of contraband and aliens.
3. Ports are open and exposed and are susceptible to large-scale acts of terrorism.

4. The current inspection levels of cargo containers are insufficient to counter potential security risks. Technology is not adequately deployed to allow for the nonintrusive inspection of cargo containers.

In addition, the United States has grown increasingly dependent on imported energy resources; any disruptions to the supply line would be detrimental to the country's consumers and economy. It is expected that America's ports will handle double the total volume of imported and exported goods in the next twenty years.²¹

In 2007, Congress passed a directive that 100 percent of U.S.-bound cargo containers be X-rayed for nuclear or radioactive substances. However, according to CBP, only 4.1 percent were scanned in 2012 when the fiscal year ended on 30 September.²² This was about the same percentage of containers that were inspected in 2007. Nothing has changed, and customs officials have given up on attaining the 100-percent goal set by Congress.²³ The findings in this research will allow both political leaders and DHS to realize the shortcomings of the current U.S. seaport protective measures against a nuclear or radiological attack by a device hidden in a cargo shipping container. In addition, it will identify the repercussions to the U.S. economy, specifically the supply line of goods and materials, if an attack were to succeed. Since 9/11, the United States has spent a large amount of money to increase its security, yet there is a continued possibility that a nuclear weapon could be smuggled into and detonated in a major U.S. seaport.

Conclusion

Domestic and international terrorist organizations remain active in the United States and around the world and are dedicated to advancing new attacks on the United States. DHS closely watches Al-Qaeda and its affiliates who have been linked to past

attempts to strike at the United States, such as the Christmas Day 2009 “underwear bomber” and the 2010 plot to send explosive packages utilizing printer ink cartridges. Acting DHS Secretary Rand Beers testified before Congress in November 2013 that “Domestic terrorism, and those individuals not inspired by foreign terrorist groups, remains a persistent threat.”²⁴ Senator Dianne Feinstein, D-California, member of the House and Senate Intelligence Committee, stated, “I think terror is up worldwide. The statistics indicate that—the fatalities are way up. The numbers are way up. There are new bombs, very big bombs, trucks being reinforced for those bombs. There are bombs that go through magnetometers. The bomb maker [AQAP’s Ibrahim Hassan Al-Asiri] is still alive. There are more groups than ever, and there’s huge malevolence out there.”²⁵ It is inevitable that the United States will face future attacks by these terrorist organizations; time will tell if they will be successful. Since 9/11, improved airport security has effectively thwarted additional attacks on the United States utilizing an airplane. Although the security of U.S. seaports has slightly increased and intentions of improving inbound screening processes have been a focus of DHS, it remains a vulnerable area that can be exploited through the use of cargo containers. There currently are not enough security measures in place to protect the major seaports in the United States. The failure of the 2012 deadline set by Congress in 2007 requiring all U.S.-bound shipping containers to be X-rayed for nuclear weapons is another setback to the solidification of American seaport security. The continued effort to acquire nuclear and radiological materials by terrorists combined with the weaknesses in U.S. seaport security provides the enemy with a course of action to forge another terrorist attack. With the U.S. national

debt at its highest in the nation's history, the impending budget cuts for all departments will further impede the ability to properly protect American seaports.

This chapter provided primary and secondary research questions with a thesis statement. The next chapter will present research sources that vary from government hearings, journals, and DHS reports to national strategic documents and documents produced by such law enforcement agencies as the Federal Bureau of Investigation and the Bureau of Alcohol, Tobacco, Firearms and Explosives. A case study of three ports within the United States, located in the Pacific Ocean, Atlantic Ocean, and Gulf of Mexico, will reveal their priorities in security and how they establish their current operating procedures.

¹Rafael Romo, Nick Parker, and Mariano Castillo, "Mexico: Stolen Radioactive Material Found," *CNN News*, December 4, 2013, <http://www.cnn.com/2013/12/04/world/americas/mexico-radioactive-theft> (accessed April 23, 2014).

²Port Security Council, *Port Security Is Our National and Economic Security: Fact Sheet* (Washington, DC: Government Printing Office, 2006), 5.

³U.S. Congress, *Public Law 107-295: Maritime Transportation Security Act of 2002*, 107th Cong., 2d sess., 2002, H. Rep. 107-777, 4.

⁴Transportation Security Administration, "Our Workforce," <http://www.tsa.gov/about-tsa/our-workforce> (accessed May 20, 2014).

⁵Stephen E. Flynn, "The Neglected Home Front," *Foreign Affairs* (September/October 2004), <http://www.mafhoum.com/press7/207P8.htm> (accessed November 22, 2013).

⁶John F. Frittelli, *Maritime Security: Overview of Issues*, Congressional Research Service Report for Congress RS21079 (Washington, DC: Library of Congress, 2003), 2.

⁷GlobalSecurity.org, "Al-Qaeda (The Base)," <http://www.globalsecurity.org/military/world/para/al-qaida.htm> (accessed May 20, 2014).

⁸U.S. Department of Homeland Security, “Department of Homeland Security Strategic Plan: Fiscal Years 2012–2016,” <http://www.hsdl.org/?view&did=700830> (accessed May 20, 2014), 2.

⁹U.S. Department of Homeland Security, “Radiological Attack: What It Is,” <http://www.dhs.gov/radiological-attack-what-it> (accessed May 20, 2014).

¹⁰United States Government Accountability Office, “Maritime Security: DHS Progress and Challenges in Key Areas of Port Security,” <http://www.gao.gov/assets/130/125051.pdf> (accessed May 20, 2014), 2.

¹¹*Ibid.*, 2

¹²*Ibid.*, 1

¹³National Security Strategy Archive, “The National Security Strategy Report,” <http://nssarchive.us> (accessed May 20, 2014).

¹⁴U.S. Department of Homeland Security, “Ten Years Later: A Stronger, Safer America,” <http://www.dhs.gov/blog/2011/09/11/ten-years-later-stronger-safer-america> (accessed May 20, 2014).

¹⁵GlobalSecurity.org, “Osama bin Laden,” http://www.globalsecurity.org/security/profiles/osama_bin_laden.htm (accessed May 20, 2014).

¹⁶Rexford B. Sherman, *Seaport Governance in the United States and Canada* (Alexandria, VA: American Association of Port Authorities, 2012), 2.

¹⁷United States Government Accountability Office, “Maritime Security,” 2.

¹⁸*Ibid.*, 1.

¹⁹*Ibid.*, 2.

²⁰U.S. Congress, *Public Law 107–295*, 4.

²¹*Ibid.*, 4.

²²Jeff Bliss, “U.S. Backs Off All-Cargo Scanning Goal with Inspections at 4%,” *Bloomberg*, August 13, 2012, <http://bloom.bg/MTFVZ1> (accessed April 22, 2014).

²³*Ibid.*

²⁴Senate Committee on Homeland Security and Governmental Affairs, *Statement for the Record, Acting Secretary Rand Beers, U.S. Department of Homeland Security*, 2013, 3.

²⁵Susan Jones, “Intelligence Chair Warns of ‘New Bombs, Very Big Bombs,’” *CNSnews.com*, December 2, 2013, <http://cnsnews.com/news/article/susan-jones/intelligence-chairs-warn-new-bombs-very-big-bombs> (accessed February 26, 2014).

CHAPTER 2

LITERATURE REVIEW

The 9/11 Commission Recommendations were implemented and passed by an overwhelming margin in the House of Representatives during the 110th Congress in October 2006.¹ Although the recommendations were primarily focused on airport security measures, they acknowledged the potential vulnerability of U.S. seaports against a terrorist attack. In 2007, Congress mandated that within three to five years all containers bound for the United States be scanned and marked with a seal. By the end of 2012, only 4.1 percent of inbound shipping containers were screened using this method, and seaport protection continues to lag behind airport security. The purpose of this thesis is to examine U.S port security, focusing specifically on the threat of shipping cargo containers as a means to transport an undetected nuclear or radioactive device through a major U.S. seaport. The research will also examine ports' standard operating procedures and protective measures against these events.

The information utilized for this chapter will come primarily from existing national and federal policies. In addition, previous policies implemented post-9/11 will be reviewed in terms of how they have evolved or changed to current policies. Private sector publications that chronicle the developing technology in support of seaport protection will be drawn on, as well as specialized think tank articles focused on maritime security. Despite evidence of a lack of seaport security, which leaves the United States vulnerable to a terrorist attack, some government-level officials believe that aviation security should remain a top priority and prudent risk has been considered when developing overall

homeland security. This chapter will demonstrate the actions (or lack thereof) and current procedures implemented by the United States to strengthen its seaport security against a nuclear or radiological attack.

Existing Publications

The U.S. government implemented numerous policies and strategies focused on strengthening homeland security after 9/11. Security and law enforcement agencies explored and considered all avenues of potential future terrorist attacks. National strategic and incident response guidance was updated or developed to detect, deter, defeat, and prepare for future attacks and now serves as a guide for all public and private sectors. From this guidance, the following documents will be used in this chapter.

Maritime Security: Progress and Challenges 10 Years after the Maritime Transportation Security Act. A report generated in 2012 to review the progress and challenges of the past ten years after the implementation of the MTSA, including security planning, port facility and vessel security, maritime domain awareness and information sharing, and international supply chain security.

Maritime Transportation Security Act of 2002. An act passed by the U.S. Senate and House of Representatives to establish a program to ensure greater security of U.S. seaports, among other purposes.

National Defense Strategy. A document issued in 2008 by the Chairman of Joint Chiefs of Staff as a deliverable to the Secretary of Defense that briefly outlines the strategic aims of the armed services and how they will support the President's National Security Strategy.

National Maritime Domain Awareness Plan for National Strategy for Maritime Security. This 2013 document provides the framework for collaboration to appropriately share and safeguard information within the Global Maritime Community of Interest to position decision makers to prepare for, prevent, respond to, and recover from a broad spectrum of potential maritime threats.

National Response Framework. Now in its second edition, this 2013 framework offers a guide to how the United States conducts all-hazards response. It is built on scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities across the nation, linking all levels of government, nongovernmental organizations, and the private sector. It is intended to capture specific authorities and best practices for managing incidents that range from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters.

National Strategy for Maritime Security. Created in 2005 to align all federal government agencies involved in maritime security programs and directives into one national effort involving the appropriate federal, state, local, and private sector entities. The supporting plan pertinent to this study is the Maritime Transportation System Security Plan, which provides an outline to meet the current and evolving changes in maritime threat.

2012–2016 Border Patrol Strategic Plan: The Mission: Protect America. A strategic plan that establishes an approach for the Border Patrol that is tailored to meet the challenges of securing a twenty-first-century border against a variety of threats and adversaries.

U.S. National Security Strategy. A document prepared in 2010 by the executive branch of the U.S. government for Congress that outlines the major national security concerns and how the administration plans to deal with them.

These published national strategies, as well as documentation from DHS, the Federal Emergency Management Agency (FEMA), the Department of Justice, and private security corporations, will support this thesis and provide a better understanding of the goals, guidelines, plans, and policies of the United States toward maritime security. The information shared here will focus on maritime security implementation post-9/11 and the importance of cross-talk and cooperation between federal departments and the agencies that fall under them. Most important will be the ability to implement new seaport security strategies in the state, local, and private sectors.

National Strategies and Plans

In 2010, President Obama's administration published the U.S. National Security Strategy, which outlined several national interests.²

1. Security: The security of the United States, its citizens, and U.S. allies and partners.
2. Prosperity: A strong, innovative U.S. economy in an open international economic system that promotes opportunity and prosperity.
3. Values: Respect for universal values at home and around the world.
4. International order: An international order advanced by U.S. leadership that promotes peace, security, and opportunity through a stronger cooperation to meet global challenges.

These interests are linked to one another and must be pursued together, not as individual interests. The threats facing the United States have changed in the last twenty years and now include the spread of nuclear weapons to extremists aimed at destroying the American people's way of life. The security at home will rely heavily on the systems already in place to prevent and deter attacks. To date, the 2010 strategy remains in effect with the current administration.

The United States remains committed to safeguarding all Americans against terrorism, disallowing the establishment of a terrorist safe haven, and preventing terrorists from obtaining or using WMD. The United States will not tolerate or accept the possibility of a terrorist organization acquiring nuclear technology. The nation's security and stability will always be linked to the security and stability of the world.

The National Response Framework³ is required by, and integrates under, a larger National Strategy for Homeland Security⁴ that serves to guide, organize, and coordinate homeland security efforts. This strategy reflects the increased understanding of the threats confronting the United States and incorporates lessons learned from exercises and real-world catastrophes. It provides a common framework by which the United States should focus its homeland security efforts on achieving four goals.⁵

1. Prevent and disrupt terrorist attacks.
2. Protect the American people, critical infrastructure, and key resources.
3. Respond to and recover from incidents that do occur.
4. Continue to strengthen the foundation to ensure long-term success.

This strategy is supported by a solid communication plan developed by DHS for future incidents as illustrated in figure 1.

The nation's leadership holds U.S. security as its number one priority and has implemented a strategic plan to be executed by multiple agencies. The report from the Government Accountability Office on the review of the MTSA 2002 is the primary document that will be used to determine the effectiveness of the plan and its continued challenges.⁶

Key Maritime Acts

The establishment of a national strategic plan and its synchronization and coordination with all levels of government was the first step in achieving an effective security operation for the nation's seaports. President Bush signed the MTSA in November 2002, which required a wide range of security improvement designs to include monitoring and training to help protect the nation's seaports, waterways, and coastal areas from terrorist attacks. It also required the federal government to address vulnerabilities and specific requirements for handling inbound international shipping cargo. In addition, President Bush requested \$57 billion from Congress to support homeland security initiatives, of which only \$2.3 billion was allocated to seaport security.⁷

On 13 October 2006 the SAFE Port Act, a companion to the GreenLane Bill to improve security at U.S. seaports, was approved and signed by Congress. This act authorized nearly \$3.4 billion annually over five years for improving port security and another \$400 million annually over five years for additional grants and training exercises

for its major seaports. The bill also required that all major seaports, which handle 98 percent of all cargo containers bound for the United States, be scanned for radiation detectors by the end of 2007.⁸

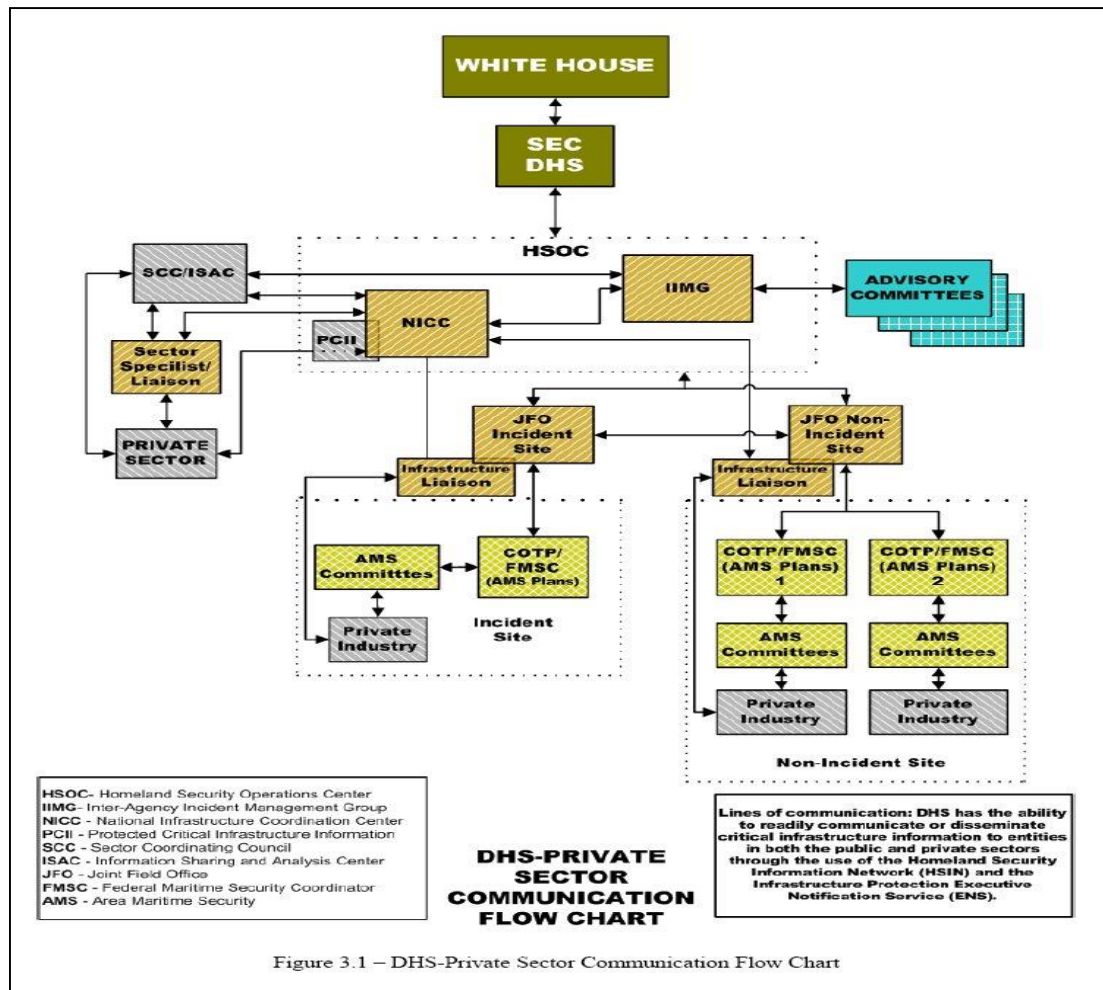


Figure 1. Department of Homeland Security Communication Flow Chart

Source: U.S. Department of Homeland Security, *Maritime Security Infrastructure Recovery Plan for the National Strategy for Maritime Security* (Washington, DC: Government Printing Office, 2005), 21.

In addition, DHS was mandated to establish a pilot program at three foreign ports to test new technology developed for nonintrusive cargo inspection.⁹ This bill led to the implementation of the 9/11 Commission Recommendations passed by the House of Representatives requiring that 100 percent of all U.S.-bound containers be scanned and marked with a seal as part of improved port security measures.

Through CBP, the Container Security Initiative was established and implemented in the cargo security strategy. This initiative directly addresses the potential terrorist threat to U.S. border security and global trade through the use of a maritime cargo container by deploying a multi-specialty team to foreign ports in which cargo containers are shipped to the United States (see figure 2). Since January 2002, this initiative has been implemented in fifty-eight ports worldwide, representing the highest volume of containers shipped to the United States.¹⁰

These legislative acts and initiatives made great strides in establishing strong and effective seaport security. However, these directives must be executed by trained personnel with the use of proper technology. In addition, compliance by the private sector with the new regulations must be ensured. Unfortunately, even with these laws in effect, they do not address all of the seaport security issues. Additional attention must be focused on improving scanning processes at the port of embarkation, designing and implementing technology to enable 100-percent container screening, and building cooperation and collaboration between the government and private sector to dictate the continuous flow of commerce through U.S. seaports.

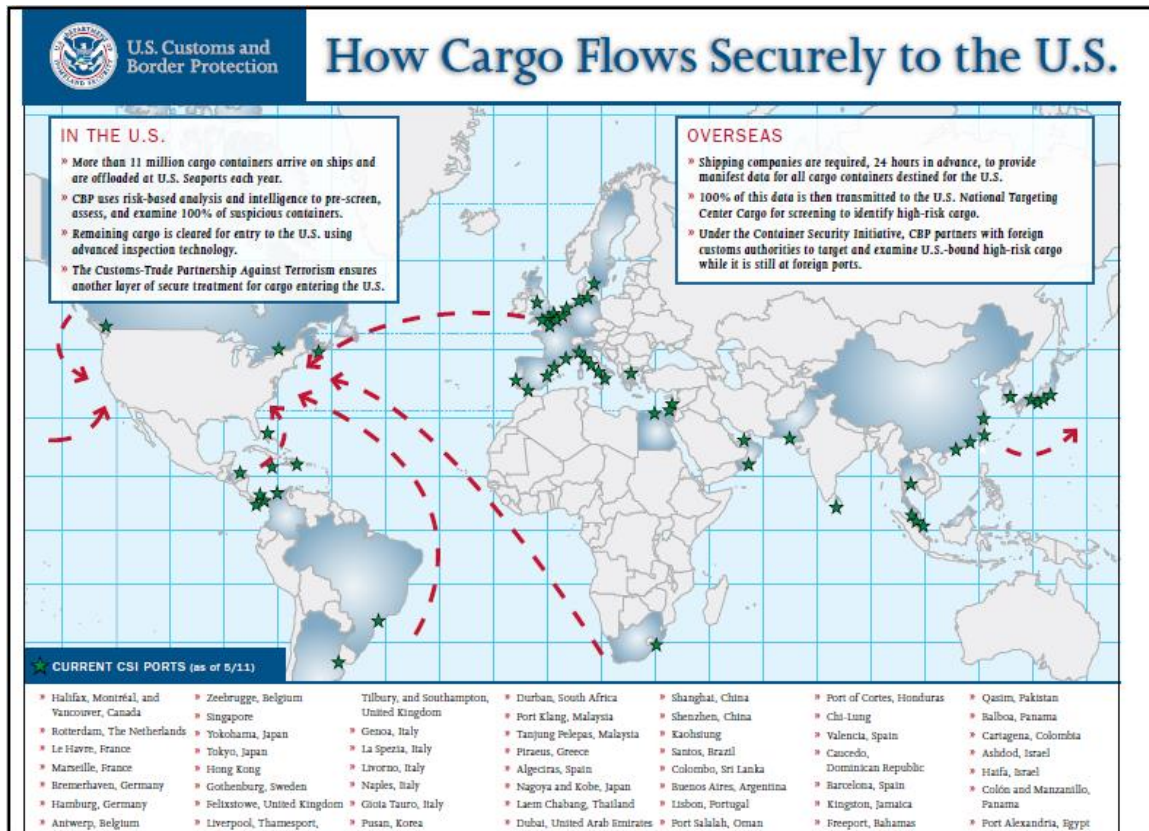


Figure 2. U.S.-Bound Cargo Flow Chart

Source: U.S. Customs and Border Protection, *Container Security Initiative in Summary* (Washington, DC: Government Printing Office, 2011), 3.

Private Sector Think Tanks and Reports

This thesis will rely heavily on current government strategies, guidelines, and plans. However, think tank reports and studies conducted by universities and the private sector will provide an outside look at the current posture of U.S. seaport security. All can agree that the United States remains vulnerable to a terrorist strike and that the nation's seaports remain a viable target for a nuclear attack. Several subject matter experts want to refocus on establishing tighter security regulations with trading partners, fully knowing

that 100-percent inspection cannot be attained.¹¹ This will allow the security responsibility to be shared with international partners. Others feel that increasing seaport security measures will impact the economy, not only for the United States but for the entire international community.¹² Possibly the most important is the view of funding and resources allocated to seaport protection and whether the grants provided by FEMA are adequate enough to assist in the prevention of a terrorist attack.

Challenges

More than 27 percent of the U.S. gross domestic product is accounted for via overseas trade. Maintaining the right balance between establishing a rigid security program and a consistent flow of goods through U.S seaports is critical. The security process must not be so stringent that it will affect the national or international economy or so flexible that it will be exploited by terrorists for its vulnerabilities. The key will be a partnership between the government and the private sector where the establishment of clear guidelines will minimize the cost to private companies that comply with government regulations, while also providing government grants and benefits to corporations that make an effort to improve the security program.

The Government Accountability Office report on the ten-year review of the MTSA 2002 identified several challenges that have hindered the implementation of maritime security programs. These challenges were determined by DHS during its program review.¹³

1. Program management and implementation: The urgency to implement security processes negatively affected the management of some programs. DHS learned

that state and local governments, federal agencies, and private sectors did not have an adequate strategic or workforce plan for the initial security program.

2. Partnerships and collaboration: DHS discovered that its interagency partnerships were limited due to a lack of information-sharing capability, which slowed maritime domain awareness.
3. Resource, funding, and sustainability: The economic constraints derived from increased security costs caused DHS to allocate resources to sustain security programs other than the maritime domain.
4. Performance measures: Lack of reliable data collected by DHS and its interagency partners resulted in an inaccurate performance evaluation of the maritime security plan.

Although some of these challenges are currently being rectified, much work needs to be done at all levels of government, including the private sector. The overall assessment of the program's effectiveness is to ensure that the nation continues to improve and strengthen U.S. seaport security against risks associated with potential terrorist attacks.

Failure to Achieve Directive

At the end of fiscal year 2012, the Obama administration failed to meet the deadline imposed by Congress in 2007 that all shipping containers be scanned with an imaging and radiation detection device before they reach the United States. Former DHS Secretary Janet Napolitano informed Congress of the need for a two-year extension due to the cost of the project. During her testimony, she stated that it would cost nearly \$16

billion to fully implement radioactive scanners in approximately 700 seaports worldwide that ship to the United States.¹⁴ DHS relies heavily on intelligence provided by multiple federal agencies to identify high-risk containers that require a more thorough check. Although the system currently in place has resulted in narcotics and illegal materials confiscation, there have been no reports of smuggled nuclear material. It is important to note that nearly 99 percent of the containers departing a U.S. seaport and heading to their final destination in the United States are monitored for radiation; however, if cargo of this type reaches the U.S. mainland, it has already met its goal by passing through the security measures prior to arriving in a U.S. seaport.¹⁵

Conclusion

This chapter established the strategy, policy, and plan for U.S. seaport security that forms the basis of this analysis. Since 9/11, several legislative acts have provided security guidelines and frameworks for federal, state, and local governments, as well as the private sector. Progress in the areas of collaboration and data and intelligence gathering among federal agencies has improved, and existing application of government assets to combat a terrorist threat exhibits a measure of success. However, the failure to meet Congress's 2007 directive of 100-percent cargo container scanning means the nation's seaports are not fully protected from a nuclear device. In addition, federal agencies believe that attaining the 100 percent goal is not only unrealistic but cost prohibitive.

A case study analysis of three different seaports in the United States will frame the guidelines, policies, and plans for this thesis. Current and former agency leaders will

provide their thoughts on the subject. In addition, think tank corporations and universities will offer their own view of the matter as well as recommendations. The next chapter will cover the research methodology utilized to obtain and compare data on the chosen seaports that will be used for analysis.

¹House of Representatives, *Improving America's Security Act of 2007: H.R. 1*, 110th cong., 1st sess., 2007, 1.

²Executive Office of the President of the United States, *National Security Strategy*, May 2010," <http://nssarchive.us/NSSR/2010.pdf> (accessed January 22, 2014), 7.

³U.S. Department of Homeland Security, *National Response Framework*, 2nd ed., http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf (accessed February 26, 2014).

⁴Homeland Security Council, *National Strategy for Homeland Security*, http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (accessed January 22, 2014).

⁵*Ibid*, 1.

⁶United States Government Accountability Office, "Maritime Security: Progress and Challenges 10 Years after the Maritime Transportation Security Act," <http://www.gao.gov/assets/650/647999.pdf> (accessed January 22, 2014).

⁷Congressional Port Security Caucus, *A Report on Port and Maritime Security: An Agenda to Enhance America's Security* (Washington, DC: Government Printing Office, 2007), 2.

⁸*Ibid*, 3.

⁹United States Government Accountability Office, "Supply Chain Security: Container Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning," <http://www.gao.gov/assets/590/588253.pdf> (accessed May 20, 2014), 4–5.

¹⁰U.S. Customs and Border Protection, "CSI: Container Security Initiative," <http://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief> (accessed May 20, 2014).

¹¹Michael Chen, “Development in Maritime and Supply Chain Security,” <http://www.iaphworldports.org/LinkClick.aspx?fileticket=x8Wf2KcuFD0%3D&tabid=5609> (accessed February 26, 2014), 31.

¹²Maritime Transport Committee, “Security in Maritime Transport: Risk Factors and Economic Impact,” [http://www.oecd.org/sti/transport/maritimetransport/18521672 .pdf](http://www.oecd.org/sti/transport/maritimetransport/18521672.pdf) (accessed January 22, 2014), 1.

¹³United States Government Accountability Office, “Maritime Security,” 16–25.

¹⁴Douglas Frantz, “Port Security: U.S. Fails to Meet Deadline for Scanning Cargo Containers,” *The Washington Post*, July 15, 2012, http://www.washingtonpost.com/world/national-security/port-security-us-fails-to-meet-deadline-for-scanning-of-cargo-containers/2012/07/15/gJQAmgW8mW_story.html (accessed January 22, 2014).

¹⁵*Ibid.*

CHAPTER 3

RESEARCH METHODOLOGY

The previous chapter reviewed the standard literature utilized for this thesis, including an array of seaport security articles published by DHS, think tank reports from academia and the private sector, national strategic documents encompassing interagency dealings with maritime security, Government Accountability Office reviews, and passed legislations. The purpose of this thesis is to examine the threat of an undetected nuclear device (to include a dirty bomb) hidden in a cargo shipping container arriving in a major U.S. seaport. It is important to note that a similar study was conducted by a Command and General Staff College student in 2009, but its focus was on a chemical or biological weapon entering the United States, not a nuclear or radiological device. Since then, no other topic has been comparable to this thesis. The first step in this research analysis was to determine National Security Strategy and DHS policies, which were identified in the previous chapter. These documents established a standard from which the evaluation criteria were developed and can be measured against. Research into these documents also produced an overview of the current policies and required protective measures passed by Congress. In addition, the examination of newspapers, magazines, and topical websites located the most current information in the area of seaport security against a nuclear device. All information acquired will be unclassified due to the nature of the research and will rely solely on public information and the analysis of subject matter experts in the field of maritime security. This chapter will establish the information required to answer

the primary thesis question and focus on the evaluation criteria used throughout the research process on three major U.S. seaports.

Background

The method of research specific to this thesis is the examination of three major U.S. seaports, one residing in the Atlantic Ocean, another in the Pacific Ocean, and the last in the Gulf of Mexico. These three ports were chosen due to their location; they also allow the study to remain unbiased toward one coast and balanced when establishing evaluation criteria. In addition, these seaports are some of the busiest in the United States and are large enough that documentation exists to conduct the study. Knowledge of the current National Security Strategy, interagency plans, and deadlines established from the post-9/11 Commission Recommendations is critical in order to conduct the case study of these three seaports. A comprehensive review and comparison of the seaports' security plans will determine if they are in compliance with current policies and linked to the National Security Strategy.

Evaluation Criteria

It is feasible and highly recommended to evaluate seaports found in different parts of the country, and this research will review three major seaports located on three sides of the United States. The case study will be based on numerous criteria that focus on the primary and secondary thesis questions, with each criterion concentrated on answering the primary question as follows: What are the current standard procedures for inbound cargo inspections in U.S. seaports, and which actions have been taken to meet the 2007

congressional directive for 100-percent inspection of weapons-grade nuclear and radioactive substances prior to departure from foreign seaports?

Table 1 provides the framework for the criteria that will be used to examine each port and to determine if the security procedures have been met. The following discussion explains each criterion in more detail.

Seaport Security Plans

1. Local plans: Within each state and county the local government will be responsible for periodically establishing a plan of action and updating it as needed. The plan must be flexible and consistent with the given federal guidelines.
2. Partnerships: Local governments and private sectors will establish an understanding and develop a partnership to create a system of checks and balances protocols that meet federal guidelines.
3. Private sectors: Commercial entities will be responsible for the shipping security of their goods via use of federal guidelines. Each private sector will ensure it is in compliance with both federal and local government policy.
4. Communication: Information sharing between stakeholders occurs at all levels. Private and public sectors, as well as local and federal government agencies, share timely and current information involving seaport security.
5. Physical security and access control: Approved physical security procedures, along with proper access control, is implemented in the seaport, periodically updated, and checked for vulnerabilities.

Table 1. Blank Case Study Comparison Chart of the Ports of Long Beach, Houston, and Miami-Dade			
Evaluation Criteria	Port of Long Beach	Port of Houston	Port of Miami-Dade
Seaport Security Plans			
Local plans written			
Local plans follow strategic guidance			
Local government partners with private sector			
Communication system in place			
Physical security and access control			
Application of Guidelines			
Applied federal guidance within local plans			
Applied legislation within local plans			
Scheduled exercises conducted by local public and private sectors			
Exercises met federal standards			
Training conducted			
Federal Funding			
Applied for federal grants			
Budget allocated for technology research and development			
Budget allocated for infrastructure improvement			

Source: Created by author, adapted from Jenifer L. Breau, “Seaport Protection Against Chemical and Biological Attacks” (Master’s thesis, U.S. Army, Command and General Staff College), 62.

Application of Guidelines

1. Application of policy: Federal and local government plans incorporate and implement the national strategic guidance established in national plans and legislations.
2. Exercises: In partnership with the private sector, the local government conducts periodic exercises to validate the security of the current plan. Partnerships and coordination occurs among organizations within DHS such as FEMA, CBP, and the United States Coast Guard (USCG). These organizations validate security plans at the state and local levels.
3. Training: In addition to periodic exercises, training programs must be incorporated into local plans, including internal training for all levels of personnel. External programs for partners and outside agencies are usually made available by local government.

Federal Funding

1. Grants: FEMA administers grant programs to improve the security of the nation's highest risk port areas. These grants can be used to improve infrastructure security and upgrade technology.
2. Budget for technology research and development: Due to the limited technology available to properly screen nuclear material inside cargo containers, funding for research and development is necessary to attain or develop technology that can enhance port security.

3. Budget for improved infrastructure: Current infrastructure must be periodically overhauled to update aging security mechanisms and inadequate security processes and procedures in order to meet current security standards.

Conclusion

This chapter established the criteria that will be used to evaluate the three seaports: existing seaport plans in the local and private sector, the application of guidelines, and the federal funding received to assist security efforts. Each evaluation criterion will uphold the thesis statement and support the understanding of the case study. In addition, the criteria for each port will be examined to ensure it is compliant with and follows the guidance set by the federal government. This also includes funding of seaport security projects as well as federal grant requests. The chosen ports' compliance status will be presented in the next chapter, along with answers to the primary and secondary questions.

CHAPTER 4

ANALYSIS

The research methodology and process to be used for this study was provided in the previous chapter. The 2010 National Security Strategy was used as an initial starting point, leading to additional government documents and websites of federal agency stakeholders in maritime security. Private sector perspectives were also reviewed through articles and think tank reports that exhibited an array of ideas and courses of action to improve seaport security. A research matrix was developed to provide evaluation criteria for the three ports chosen for the case analysis. The purpose of this thesis is to examine the ability of U.S. seaport security to deter and defeat a nuclear or radioactive device hidden in an inbound cargo shipping container. This chapter reviews federal and local government responsibilities, to include the private sector. In addition, monitoring oversight, current procedures, and technology use as preventative measures will be analyzed. An overview of the three ports used in the case study will be provided, and the evaluation criteria established in the previous chapter will compare the three.

Primary Research Question

The primary question of this thesis is: What are the current standard procedures for inbound cargo inspections in U.S. seaports, and which actions have been taken to meet the 2007 congressional directive for 100-percent inspection of weapons-grade nuclear and radioactive substances prior to departure from foreign seaports? This chapter will provide the analysis and answers to this question.

Secondary Research Questions

The following subordinate questions were established in order to answer the primary question.

1. If standards have been improved since the MTSA 2002, will they detect and prevent a nuclear dirty bomb device from reaching a major seaport?
2. What current technology is available to screen a higher percentage of cargo containers bound for the United States?
3. Is the United States—specifically DHS—prepared for future terrorist attacks originating from inbound cargo containers?
4. Is it feasible to conduct 100-percent inspection of all U.S.-bound cargo containers?

The answers to these questions will provide further detail regarding the process and execution of U.S. port security and reveal its true effectiveness in deterring a nuclear device from detonating in a seaport.

Federal Government Responsibilities

In March 2011, the Presidential Policy Directive 8 / PPD-8: National Preparedness was released with the intended goal of strengthening U.S. resilience against external and internal threats that could debilitate the nation's security.¹ The directive recommends a series of five preparedness mission areas—prevention, protection, mitigation, response, and recovery—including the development of policy and planning documents by DHS for interagency partners, as well as state and local governments, to ensure an enhanced national preparedness. This framework addresses the key roles and

responsibilities of community leaders, nonprofit entities, and nongovernmental organizations; the private sector; critical infrastructures; governments; and the nation. The mission areas are designed to work in conjunction with the continued coordination among the departments and federal agencies focused on preventing, protecting, mitigating, responding, and recovering from threats or hazards to the United States.

The aftermath of 9/11 allowed multiple departments (DHS, the Department of Justice, and the Department of Defense) and an array of agencies under them to become actively involved in securing U.S. seaports. However, DHS remains the federal government agency largely responsible for port security. DHS is focused on preventing terrorists from entering or remaining in the United States, and its top priority is preventing the introduction or importation of WMD and nuclear grade material through homeland screening, search, detection, and interdiction. DHS coordinates its activities with partner agencies at the state and local government levels. Under DHS, the primary federal agencies involved in seaport security include USCG, CBP, and TSA. In addition, the Maritime Administration was established in 1950 with a mission to improve and strengthen the U.S. marine transportation system to meet economic and environmental security.² Although not directly related to port security, Maritime Administration maintains the Ready Reserve Force, a fleet of cargo ships used to support the deployment of U.S. military forces overseas and in national emergencies. The two lead agencies responsible for seaport security are CBP and USCG. Combining these federal agencies has been a sought-after proposal since the 9/11 Commission. Although it would streamline the duties and responsibilities for a single agency, along with standardizing

security procedures, there are challenges that will hinder its success. Funding, standards, and collaboration between the current federal agencies will impede the implementation of security procedures.

The CBP port of entry operational vision is to “secure ports of entry where potential violators are deterred; threats and inadmissible people, goods, and conveyances are intercepted; legitimate trade and travel are facilitated; and operations and outcomes are consistent.”³ This vision links directly to four DHS strategic goals: (1) preventing terrorism at ports of entry, (2) unifying as one border agency, (3) facilitating legitimate trade and travel, and (4) protecting America and its citizens.⁴ Figure 3 shows the CBP mission and the strategic framework goals for securing America’s borders.

Whereas CBP is primarily responsible for the inspection of inbound cargo, including sea containers, passengers, and ship crewmembers, USCG is responsible for the screening, evaluation, boarding, and inspection of inbound commercial ships as they approach U.S. maritime territory. They also assist in the protection of U.S. ships in port and countering terrorist threats against U.S. seaports. The Maritime Domain Awareness initiative was developed after 9/11 to allow USCG to enhance the effectiveness of its approach in evaluating terrorist threats.⁵ It consists of improved real-time shipping and carrier information to allow USCG to recognize and identify legitimate shipping vessels flowing into U.S. seaports. The initiative was developed with the assistance of other government agencies and intelligence and collection assets. Figure 4 shows the partnership between agencies and private sector entities involved with ports of entry. This partnership is responsible for daily port operations, security, and policy implementation.

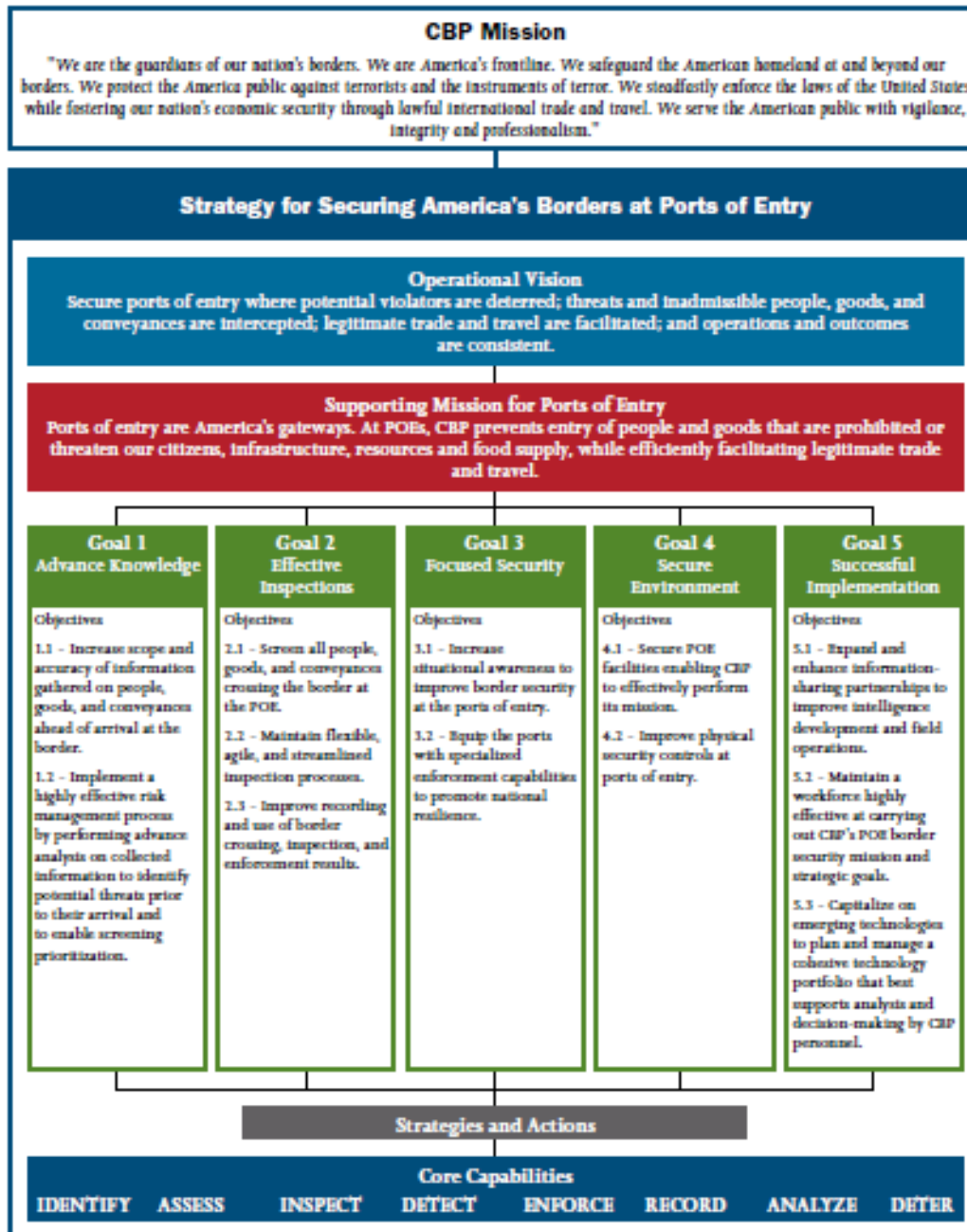


Figure 3. Strategic Framework for Securing America's Borders at Ports of Entry

Source: U.S. Customs and Border Protection, *Securing America's Borders at Ports of Entry* (Washington, DC: U.S. Government Printing Office, 2011), 4.

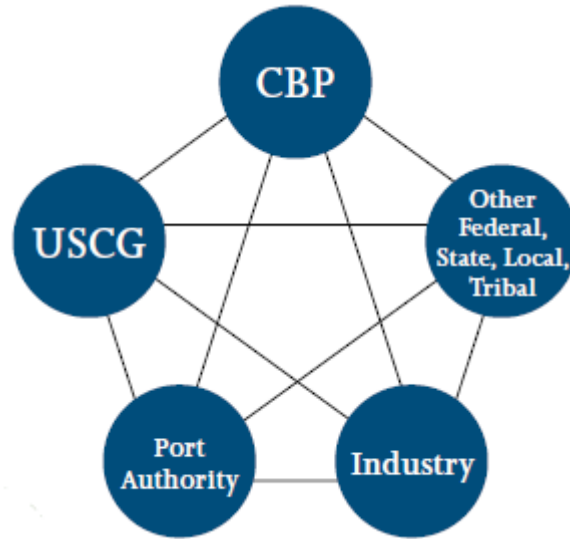


Figure 4. Partnership Relationship Diagram at the Ports

Source: U.S. Customs and Border Protection, *Securing America's Borders at Ports of Entry* (Washington, DC: U.S. Government Printing Office, 2011), 20.

As stated earlier, proposals have been generated to merge and consolidate the federal agencies responsible for seaport security. This will prevent the overlapping of efforts by different organizations and identify loopholes in the current security process that may have been overlooked. If approved and implemented, this consolidation will affect the thousands of people currently employed in these efforts and force them to change how they conduct their daily business from what they have grown accustomed to.

The United States President is the nation's leading authority to direct the federal government and its agencies to prevent and prepare for acts of terrorism. Coordinated effort and cooperation with state, local, and private sector leadership will be needed to ensure this threat is met. The federal government is responsible for the development of programs with updated regulations to meet the current policy, as well as assisting with

the funding, research, coordination, and implementation of these programs at the local, state, and government levels.

State Government Responsibilities

The state government supplements additional resources to support local governments in their efforts before, during, and after an act of terrorism. These include the direct support of city, county, and intrastate region activities. States will also administer federal homeland security grants to local communities to help strengthen their ability to prevent acts of terrorism within their communities. The governor is responsible for the public safety and welfare of the state's residents and ensures that state resources are available to respond to all types of incidents. To assist the governor, the state homeland security advisor and other state departments and agencies develop plans and internal policies to meet federal regulations as the governor sees fit. They typically work in close coordination with their federal partners in their respective fields.

Local Government Responsibilities

The local government is the first line of defense in preventing a terrorist strike. Local government officials are responsible for the safety and welfare of the people who live within their jurisdiction, just as the state's responsibility is the same. The local law enforcement agency is the lead organization that is actively engaged with the community, private industry, and state and federal agencies to identify and prevent terrorist threats. The chief elected or appointed officials have a clear understanding of the local government emergency management processes and capabilities to combat different types of hazards.

Private Sector Responsibilities

Although the private sector has a limited role in the development of security procedures set by the government, it plays an important part in preventing terrorism in a U.S. seaport by being vigilant in its day-to-day business operations and reporting terrorism-related information to local law enforcement. The private sector can further assist in implementing its own internal security procedures in conjunction with the federal mandatory regulation to strengthen security. Just as important, there will be a heavy reliance on the private sector to help establish and assist with a new normal in the community if an incident occurs.

Providing and Monitoring Oversight

During the 113th Congress on January 3, 2013, a committee was established that adopted an oversight plan for DHS.⁶ The committee will continuously monitor and assess external threats to U.S. citizens and national interests ranging from Al-Qaeda to emerging state and non-state actors determined to cause catastrophic events in the United States. The committee will also examine the capabilities and efforts of DHS and its agencies to identify, prevent, deter, and respond to emerging future threats. The committee will assess the ability of federal agencies to secure both U.S. land and maritime borders, to include personnel, technology, infrastructure, and coordination.

On the topic of port and maritime security, the 113th Congress specifically focused on port facility security; the screening of vessels, passengers, cargo containers, and crew for potential hazards or terrorist contraband and weapons; nuclear detection

efforts and the technology utilized; and the development of an approved international security standard for shipping.⁷

Current Regulations, Policies, and Programs

33 Code of Federal Regulation Subchapter H – Maritime Security

33 Code of Federal Regulations Subchapter H covers the updated regulations on maritime security. Its purpose is to implement the mandated changes and updated regulations required by the MTSA 2002. This subchapter is categorized by five subparts (A through E), stating the purpose, new DHS alignments, preparedness, and execution of the communication, security, and assessment planning.⁸

33 U.S. Code § 1226 – Port, Harbor, and Coastal Facility Security

This code identifies the authority of the DHS secretary and the actions he may take in order to prevent or respond to a terrorist attack. This subsection states the required measures to conduct harbor and port patrols; USCG inspections, recruitment, and training; and the techniques for preventing or responding to acts of terrorism.⁹

MTSA 2002

The MTSA 2002 originated after the 9/11 attacks on the United States and was designed to deter or respond to an attack on a U.S. seaport.¹⁰ This act forced a unit of effort among existing agencies responsible for U.S. maritime security, specifically USCG, TSA, CBP, and Maritime Administration. This enabled USCG to garner a large law enforcement responsibility in seaports with continuous coordination with TSA and CBP. Also mandated was the creation of new security programs and delineation of

responsibilities among the agencies involved. In addition, required security assessments, procedures, and regulations were developed under this act, to include the authorization of the Transportation Worker Identification Credential Program, Targeted Infrastructure Protection Program, and Port Security Grant Program.

Customs-Trade Partnership Against Terrorism

The Customs-Trade Partnership Against Terrorism, also known as C-TPAT, was developed in November 2001.¹¹ Its focus is to protect the world's trade industry from terrorist attacks, allowing continuous economic transactions between the United States and its trade partners. The partnership is between CBP and private industries, normally shipping companies, that agree to work with CBP to protect their supply chain. The initiative involves identifying security gaps and implementing mandated security measures and best practices. In addition, the company provides CBP with an opportunity to assess current security measures and make recommended changes if required. Compliant members of this partnership allow their shipments to be designated as low risk and will be less likely to be examined, thus allowing the continuous free flow of goods into the United States with minimum time delays. Today, there are more than ten thousand certified partners from around the world in the trade community that have been accepted into the program and are reaping the benefits of their additional efforts.¹²

Container Security Initiative

The Container Security Initiative (CSI) was implemented in 2002 and meant to be the counterpart to the C-TPAT program because of its focus on the supply chain security of cargo containers originating from designated international seaports.¹³ This initiative

allows partnerships between deployed CBP officers and their foreign counterparts to detect and deter potential hazardous containers that may be delivering WMD. Prior to loading a container on board a vessel destined for the United States, each container is inspected utilizing radiation scanning technologies. At present, there are fifty-eight participating countries, accounting for 85 percent of container traffic bound for the United States.¹⁴

Operation Safe Commerce

Operation Safe Commerce was designed specifically for cargo container security.¹⁵ Initial pilot programs were started for the Ports of New York and New Jersey, Los Angeles and Long Beach, and Seattle and Tacoma. The intent was to utilize an integrated system in foreign ports composed of seals, sensors, tracking devices, and cargo information systems to detect tampered containers. The ultimate goal was to promote a productive and efficient shipping process while maintaining a secured and uncompromised sea container. Although the program has recently been terminated at designated ports due to budget shortfalls, committee members believe that this system will be necessary to secure the U.S. international supply chain, with cooperation from foreign partners.¹⁶

Maritime Administration

The Maritime Administration was established in 1950 with a mission to improve and strengthen the U.S. marine transportation system to meet the economic, environmental, and security needs of the nation.¹⁷ The administration is housed within the U.S. Department of Transportation and is responsible for maritime transportation. It

develops and institutes programs that promote the use of maritime vessels and their integration with other modes of U.S. transportation and is also involved in the areas of shipping, ship building, port operations, vessel operations, national security, environment, and safety. In addition, Maritime Administration is responsible for maintaining the operational status of the merchant marine, as commercial mariners, vessels, and maritime facilities are vital for supporting national security.

Megaports Initiative

Established in 2003, the Megaports Initiative assists major trade partners across the globe in equipping and training foreign customs, port authorities, and other related entities on radiation detection equipment and alarm communication systems.¹⁸ The intent is to enhance the detection capability for special nuclear and radioactive materials in containerized cargo moving across maritime shipping networks. This initiative collaborates closely with CBP and the Domestic Nuclear Detection Office, to include the Department of State, to counter nuclear and radiological threats against the United States and its international trade partners.

The initiative's goal is to equip and train personnel on the radiation detection system for all major seaports worldwide by 2015, with the aim of scanning as much of the container traffic as possible regardless of destination. Attaining this goal will mean that approximately 50 percent of the world's maritime sea cargo is scanned for nuclear and radiological materials. To date, there are twenty-seven operational megaports worldwide with fully installed equipment.¹⁹

Federal Grant Programs

To help U.S. seaports improve security vulnerabilities and meet the MTSA 2002 security plans, the Port Security Grant Program (PSGP) was launched in 2002 and has appropriated more than \$2 billion.²⁰ FEMA is responsible for administering grants to approved applicants; however, because USCG is the lead agency for port security, FEMA seeks recommendation from it and other maritime agencies in making appropriate grant award decisions. Awardees have used these funds to purchase an array of high-tech security systems, to include sonar sensors used in harbors, radar systems, and high-resolution cameras. FEMA allocates grant funds based on the evaluated risk of the seaport from a terrorist attack.

To establish criteria for the grant awards, FEMA developed four groups based on their risk evaluation model. Each group has a risk level designated by FEMA, with Group I serving as the highest risk port areas due to their activities and functions; these ports include Los Angeles and Long Beach, San Francisco, New Orleans, Delaware Bay, New York and New Jersey, Houston and Galveston, and Puget Sound. Group I normally receives 60 percent of the yearly appropriations, while Group II is awarded approximately 30 percent; Group III and “All Other Port Areas Group” must compete for the remaining 10 percent of the PSGP funds.

Technology Currently in Place

It is imperative to U.S. national security and economic prosperity to ensure a free flow of goods within the global supply chain. CBP launched the CSI in January 2002 in order to identify, target, and inspect high-risk cargo from foreign ports prior to departure

to the United States. However, in 2005, the Government Accountability Office reported that 35 percent of the cargo containers were not inspected at the participating ports due to limited staffing and detection or scanning equipment.²¹ In addition, CBP cannot fully assure that the inspection of containers for WMD was successful and reliable due to the limited and ineffective detection equipment.

Due to the increased funding by the PSGP in recent years, U.S. seaports have been able to expand their security through various programs and technologies. Although the latest technology assists in the deterrence of a nuclear or radiological weapon from entering the United States, it is only implemented in designated critical seaport locations, while other seaports deemed as noncritical have less complex and advanced equipment. The technologies in place are part of the multilayered approach that DHS is implementing nationally, concentrating on prevention and detection processes to improve seaport security. The following technologies have either been implemented or are in the process of being installed in the identified critical seaports.

Transportation Worker Identification Credential Program

The Transportation Worker Identification Credential (TWIC) program is a security measure mandated by Congress through the MTSA 2002 and implemented in April 2009. This program is a TSA and USCG initiative that provides and implements a tamper-resistant biometric credential to all seaport personnel, shore workers, and truck drivers requiring unescorted access to secure areas of U.S. seaport facilities and maritime vessels regulated under the MTSA 2002, including all USCG-approved and certified commercial mariners. An estimated 750,000 individuals require this program.²² Personnel

seeking unescorted access to secure areas aboard designated vessels, and all USCG-credentialed merchant mariners, must obtain these credentials. To do so, an individual must provide biographic and biometric information such as fingerprints, sit for a digital photograph, and successfully pass a security threat assessment conducted by TSA. Being able to control access to secure areas is critical to enhancing port security.

Radiation Portal Monitors

Radiation Portal Monitors are passive radiation detection devices originally used to screen individuals, vehicles, cargo, or other objects for illegal materials and/or substances at borders or secured facilities. However, after the 9/11 attacks, the fear of terrorist strikes with radiological weapons expanded the role of these monitors to include the scanning of inbound sea cargo containers in the United States. CBP started the Radiation Portal Monitor program for all U.S. borders (land, sea, and air) to detect radiation emanating from an object passing through the scanning process. The monitors are playing an increasing role in the DHS multilayered strategy to deter terrorist threats. The Domestic Nuclear Detection Office reported that there are currently 444 Radiation Portal Monitors operating throughout U.S. seaports, thus meeting the requirement to screen all containerized cargo at the twenty-two seaports with the most container volume.²³

Vehicle and Cargo Inspection System

Another initiative implemented by DHS to support its multilayered strategy, the Vehicle and Cargo Inspection System utilizes X-ray technology to produce images of tankers, commercial trucks, sea and air containers, and other vehicles for contraband such

as drugs, weapons, and currency.²⁴ This system complements the Radiation Portal Monitors by allowing the inspection of a cargo container by moving the technology over the stationary vehicle containing the cargo. However, this is a time-consuming screening method and drastically slows the inspection process.

Radio Frequency Identification Devices

Radio Frequency Identification Devices are a new type of electronic seal that serves as a tracking device in the global supply chain network.²⁵ The device is fastened and/or installed to a cargo shipping container's latch and continuously collects and transmits data without human intervention. This procedure is concurrently utilized as part of the C-TPAT program.

Anti-Tamper Seals

Anti-tampers seals are reliable and inexpensive intrusion detection technology utilized to increase transparency for cargo shipments. Advanced seals provide CBP with necessary information on cargo prior to arrival in a U.S. seaport.

Case Study of Houston, Long Beach, and Miami-Dade Seaports

The three ports selected for the case analysis are Port of Miami-Dade located in Florida, Port of Long Beach located in California, and Port of Houston located in Texas. Each port is situated along a major coastline: the Atlantic Ocean, the Pacific Ocean, and the Gulf of Mexico, respectively. Port of Long Beach and Port of Houston are both categorized in Group I, designated as the highest risk ports by FEMA, while Port of Miami-Dade is categorized in Group II, having the second highest risk group. In addition,

each port has a different population size and a specific economic importance for the country if attacked with a nuclear device. Lastly, they each have enough non-classified data to conduct the research and analysis. The ports will be compared to one another using the evaluation criteria chart presented in Chapter 3, thus allowing a better view of their effectiveness.

Port of Houston Authority

The Port of Houston Authority (PHA) is one of the more modern U.S. seaports and is located on the outskirts of Houston, Texas, the fourth largest city in the United States. The port lies in a twenty-five-mile complex, where both public and private facilities are situated, and is the largest petrochemical complex in the nation and the second largest in the world. In terms of overall annual foreign tonnage (200 million tons of cargo move through PHA, transported by more than 8,000 maritime vessels and 200,000 barge calls), PHA is the second busiest in the United States and thirteenth busiest in the world and is responsible for more than 2.1 million jobs. Approximately 25 percent of the oil imported to the United States is transported by oil tankers for processing into gasoline by PHA's refineries, to include the largest refinery in the United States with the ability to produce 567,000 barrels a day. In addition, PHA is categorized by FEMA as Group I, a high-risk port.

PHA's top priority is the security and safety of the personnel who work at the port, as well as the surrounding communities. This includes the facilities that support the port directly and indirectly, thus making PHA the main economic source for Texas. The port's vision statement encompasses seven key objectives, one of which is its

commitment to security: “Work with public and private partners to provide secure facilities for the community, for our customers, businesses, and employees, and for the others who work and visit here.”²⁶

PHA owns, oversees, and operates the port’s eight public terminals. Due to the state’s Sunset Advisory Commission’s report released in August 2012, the port was required to make changes to its operational processes.²⁷ PHA’s executive management is developing a new organizational structure that will assist in creating efficiencies and maximize profits for the port.

Seaport Security Plans and Interagency Coordination

All terminals within the PHA are regulated by USCG in accordance with the port’s Facility Security Plan (FSP) and are within MTSA 2002 guidelines and 33 CFR 105 regulations (see http://www.uscg.mil/d9/msuChicago/docs/FSP_Review.pdf for the USCG FSP used to assess all U.S. seaports). PHA works closely with all security partners at the federal, state, and local levels, to include the private industries operating from more than 150 facilities along the Houston Ship Channel. In addition to its compliance with MTSA 2002, PHA is the first port authority in the world to be certified as ISO 28000:2007, the international security standard for supply chain security. This international security standard sets strict and heavily regulated security management processes, and both private and public entities must adhere to the approved and established security practices. It took nearly three years for PHA to develop and enhance its security processes and to apply to the Port Police and its partners in maritime security to achieve this certification, which was awarded in March 2008. To meet these standards,

improvements in the training of Port Police and its security partners were required, as were enhanced security processes, procedures and policies, and technological advancements in monitoring, documentation, and efficient vehicular processing through PHA gates.

Although CBP and USCG are the two federal agencies responsible for PHA's security and safety, the port maintains its own emergency response teams: Port Police and fire departments. PHA has more than one hundred full-time police and firefighters dedicated to all eight public port terminals within PHA, thus ensuring the safety and security of all personnel and critical infrastructure. All personnel assigned to the police and fire departments are certified by the state of Texas and are required to complete annual trainings and certifications.

Application of Plans and Technology

PHA is an active member of both the C-TAT and CSI programs operated by CBP. PHA uses a layered approach to securing its territory. This approach is executed by the USCG, the Harris County Sheriff's Office, and the Houston Police Department, all of whom conduct maritime patrols along the channels. In addition, the majority of the ship channels have been designated as security zones, meaning that all unauthorized boaters are restricted from entering the channel. Although each of the eight terminals has its own security procedures, all are in compliance with the MTSA 2002 guidelines and enforced by DHS using the procedures detailed in the 33 CFR 105. Attaining a copy of the port's security plan is not possible due to its classified nature. PHA's FSP, which is reviewed, audited, and filed by USCG, is kept confidential according to the regulation detailed in 33

CFR 105. All terminals require that all port employees, tenants, ship agents, visitors, and vendors receive clearance through the TWIC program, and even then they are not guaranteed access to the port. In May 2004, with the assistance of CBP's Radiation Portal Monitoring project, PHA participated in a federally mandated cargo screening aimed at deterring nuclear and radiological materials transported inside cargo containers from being brought into the United States. To date, the port has thirty-two Radiation Portal Monitors in its complex, and all outbound containers are scanned for radiation before departing the port into mainstream U.S. waters.

PHA also has external programs and initiatives in place that work in conjunction with its FSP to ensure that the local, state, and federal governments—to include the private sector—are focused on shared mutual interests. The following major programs assist with enhancing PHA's security.

Area Maritime Security Committee. This committee was established in 2002 under the direction of the USCG captain. It encompasses both private and public entities that are affected by maritime activities and addresses PHA security issues. As a member of this committee, PHA actively participates in its subcommittees and initiatives.

East Harris County Manufacturers Association. This voluntary program consists of 125 chemical manufacturers, refineries, and supporting terminal facilities operating in PHA. This alliance addresses security issues involving the protection of petrochemicals and other hazardous materials facilities, and works closely with other security and safety agencies to prepare for future man-made and natural disasters.

Houston Ship Channel Security District. Governor Rick Perry signed the Houston Ship Channel Security District into law in 2007. This law is a public and private partnership that comprises the port terminals' major stakeholders, who work closely with their governmental entities to focus on matters of preventative and responsive security and safety. This includes mandated security assessments of the facilities, leading to funding of security initiatives for the port.

The Houston Area Maritime Operations Center is one of the newest facilities in PHA. This complex is the main operational center for all joint team and security agencies responsible for the security and safety of the Houston Ship Channel. The Houston Area Maritime Operations Center provides coordination and information-sharing capability to all agencies involved to ensure a more efficient and deliberate emergency response.

In September 2013, PHA conducted SECUREX 2013. This exercise simulated a dirty bomb to determine the effectiveness of the federal, state, local, and private sectors' security response. The exercise also confirmed the incident command system functions and their ability to effectively institute the security plan in place. More than 170 attendees from fifty different agencies participated in the annual exercise.

Federal Funding

In FY 2013, PHA was awarded nearly \$5.3 million in PSGP funds to enhance its security capabilities. During the fifth round of federal grant awards (the first round began in FY 2002), nearly \$142 million was allocated by DHS to thirty-six U.S. ports; PHA received the largest portion at nearly \$142 million, which directly funded efforts to

protect ports from small craft and underwater attacks and enhance explosive detection capabilities.

Port of Long Beach

The Port of Long Beach (PLB) is the second busiest seaport in the United States and eighteenth in the world for handling cargo containers. It resides on nearly 3,200 acres of land and handles 75 metric tons of cargo (six million per year) valued at \$180 billion annually. The seaport generates more than \$5 billion per year in U.S. Customs revenue, and \$4.9 billion in local, state, and general federal taxes from port-related trades and activities, while performing \$1 billion in trade each day. In addition, more than \$47 billion in direct and indirect business sales are brought in annually. East Asian trade partners account for more than 90 percent of the cargo shipments through PLB. Top imports include crude oil, electronics, and plastics, and top exports are petroleum bulk, chemicals, food, and waste paper. PLB is categorized by FEMA as Group I, meaning it is a high-risk port for potential terrorist attack. In a list of the top 624 potential terrorist targets in California produced and released by the California Attorney General's Office in 2003, PLB ranked third in the state.²⁸

PLB is governed by the Long Beach Board of Harbor Commissioners, which is comprised of five members appointed by the mayor of Long Beach and confirmed by the city council. Each member serves no more than two six-year terms and oversees the 350-man department. Because the port does not receive tax revenues or funding from the city of Long Beach, the port is operated like an apartment: terminals and facilities are leased to private companies who assume authority for and operational activities on the property.

Seaport Security Plans and Inter-Agency Coordination

Since 9/11, PLB has been one of the most active seaports in terms of building and improving its security plans. PLB's goals of enhancing safety and security within the port and addressing the impacts on surrounding communities in collaboration with outside agencies is widely advertised throughout the port community. PLB is a public agency operated by the Harbor Department. Along with its own Harbor Patrol and the local Long Beach Police Department, it has established a strong partnership with USCG and CBP, to include state and DHS agencies. The port has nearly twenty-six state, municipal, and private industry stakeholders operating within the Harbor Department jurisdiction, which is the port's greatest challenge. Adding to this challenge is the partnership developed with the Port of Los Angeles's own security program. Although technically two separate seaports run by different commissioners and programs, they both share an adjoining shoreline. It is inevitable that security coordination and cooperation will be required from both ports to effectively deter and respond to a terrorist attack.

Although there are security plans in place for both ports that meet the MTSA 2002 requirements, in the event that a dirty bomb detonates in one of these ports, it is expected that nearly all eighteen agencies from federal, state, county, and local jurisdictions will respond. Because of the combined size of the Port of Los Angeles and PLB, the problem would not be the ability to get onsite assistance, but to effectively coordinate all of the combined agencies. Existing federal regulations do not establish clear lines of chain of command and responsibility for an emergency response.

In addition, the recognized lack of a consistent and effective real-time port operation overview has resulted in a project called the Virtual System, which will provide

a real-time monitoring network to allow for a better common operating picture among all stakeholders and enhanced joint awareness and collaboration. In addition, the network output by this system will be consistently shared and disseminated to all interagencies involved in PLB port security to enhance and support any incident response that may arise. Future plans will direct grant funding to support this new initiative.

Attempts to obtain the USCG FSP for PLB to enhance this research was unsuccessful due to the classified nature of the information provided in the assessment. The FSP assesses both the strengths and weaknesses of the PLB security program, and the findings are available only to the USCG and the port's security team members.

Application of Plans and Technology

All stakeholders who occupy and lease terminals or other facilities within PLB must abide by the MTSA 2002 guidelines. Since 9/11, PLB has made tremendous gains in establishing a solid security program by implementing security procedures mandated by the federal government and coordinating with the two major agencies focused on its security, USCG and CBP. PLB has been an advocate and member of the C-TPAT program since it joined in February 2003. More recently, in August 2011, the PLB completed a four-year revalidation inspection by CBP that focused on the port's security program, to include technological security enhancements.²⁹ This inspection is part of the involvement in the C-TPAT program, which aims to strengthen the partnership between CBP and national seaports to ensure a safe and secure maritime supply chain. The 2011 inspection resulted not only in a passing grade, but high praise by the CBP inspection team due to the enhanced security installments made since the 2007 inspection and the

commitment of the port's senior management team to maintain strict and updated security measures throughout the complex.

Since the last inspection in 2007, PLB has maintained or improved on the following major initiatives and projects.³⁰

1. In May 2007, PLB's security division placed in full-time service two video-equipped submersible robots (worth \$30,000 each) outfitted with video, sonar, and radiation detection devices capable of five-hundred-foot depths. The introduction of this new equipment enhanced underwater surveillance capability and provides the ability to deter underwater attacks.
2. The TWIC program continues to be in effect for all personnel who work in or around PBL and require an identification card. The port works closely with TSA to ensure that all federal requirements are met within this program.
3. In 2009, PLB opened a state-of-the-art Command and Control Center, worth nearly \$20 million. The approximately 25,000-square-foot facility was built specifically for the Harbor Patrol and adjoining security partners, to include both USCG and CBP. This facility offers joint coordination and daily interaction with all security partners, thus enabling a more effective response force.
4. The port has expanded its surveillance camera network to nearly 115 high-definition cameras throughout the harbor. These cameras have the capability of monitoring up to two miles away, and some even have facial recognition. Most of the \$80,000 camera systems were paid for by the PSGP.

Although information on joint training with federal agencies is scarce, the Governor's Office of Homeland Security created a Port Security Strategy leading to an annual emergency preparedness exercise drill lasting for two days. This drill, called Golden Guardian Exercises, attracts thousands of first responders from local, state, and federal levels to practice their individual skillsets and put into effect the current emergency plan against a simulated terrorist attack on one of the major seaports in California (Long Beach, Los Angeles, Oakland, San Diego, or Redwood City). Results of the exercise will eventually determine the strengths and vulnerabilities of the security program placed on the specific port.

Federal Funding

Since 2001, PLB has been awarded more than \$120 million in grant funding. These grants have supported security initiatives for physical security enhancements, critical facility improvements, emergency management, and interagency assistance in assessment, planning, coordination, preparedness, and exercises. Even after receiving notable praise during its 2011 CBP inspection, PLB continues to spend a large amount of funding on maintaining and improving its port

The main intent of the federal funding was to assist with the MTSA 2002 mandate to improve U.S. seaport security. PLB continues to be a model for the nation on how seaport security should be established, maintained, and improved.

Port of Miami-Dade

The Port of Miami-Dade (PortMiami) sits on 520 acres and is regarded as the "Cruise Capital of the World" due to its capability to accommodate numerous major

cruise line vessels such as Carnival, Norwegian, and Royal Caribbean. In 2010, the seaport processed more than 4.1 million cruise passengers and 7.3 million tons of cargo from around the world, providing nearly \$18 billion in economic and social benefits to the southern Florida region. PortMiami is categorized by FEMA as Group II; although not labeled as a high-risk seaport, it still maintains the designation of a potential risk and is vulnerable to a terrorist strike. In addition, it serves as the eleventh largest cargo container in the United States. PortMiami is one of the most unique seaports in the world due to its ability to cater to both cruise ships and containerized cargo.

Seaport Security Plans and Interagency Coordination

PortMiami is south Florida's example of a modern seaport able to provide safety and security to its cruise line network, as well as the containerized cargo shipping industry. Since passage of the MTSA 2002, the port has implemented new safety measures without negatively impacting its daily operations. PortMiami boasts one of the most technologically advanced programs, integrating security functions, such as access control and credentialing with business processes, with permitting and accounting.

PortMiami has established relationships with both CBP and USCG to assist with the continuous improvement of port security. In addition, the port has achieved a shared and united mission goal with the local Miami police and fire departments. In 2005, the port received a seventy-five-man Maritime Security Response Team to complement existing port security structures in order to close critical port security gaps. The Maritime Security Response Team is staffed to support continuous law enforcement operations both ashore and afloat. In addition, it can maximize effectiveness in executing USCG's

Ports, Waterways, and Coastal Security operations and augmenting shore-side security at waterfront facilities. The team has the capability and resources to assist in the detection of WMD and participate in port-level antiterrorism exercises.

The state of Florida established the Domestic Security Oversight Council, which publishes the Domestic Security Annual Report. This report explains Florida's security governance structure, highlights the accomplishments of previous years' goals, and showcases the grants awarded to the state of Florida. Although a copy of PortMiami's FSP could not be attained for this research due to its classified nature, it followed the 2013 Florida Domestic Security Strategy Plan, as follows.³¹

Goal 1. Prepare for all hazards, natural or man-made, to include terrorism.

Goal 2. Prevent, preempt, and deter acts of terrorism.

Goal 3. Protect Florida's citizens, visitors, and critical infrastructure.

Goal 4. Respond in an immediate, effective, and coordinated manner, focused on the survivors and their needs.

Goal 5. Recover quickly and restore our way of life following a terrorist act or catastrophic incident or event.

These goals are shared by all federal, state, and local law enforcement agencies and entities, including CBP, the Federal Bureau of Investigation, DHS, the Federal Air Marshal Service, TSA, and USCG. PortMiami is in full compliance with federal mandates and the Florida Department of Law Enforcement security requirements.

Application of Plans and Technology

PortMiami utilizes a multi-agency layered approach to ensure safe and secure operations within its complex. CBP certified PortMiami as a C-TPAT member. This certification allows all inbound cargo containers to be processed faster, thus translating into substantial cost savings for U.S. cargo terminal partners, freight forwarders, and trucking companies. The port's FSP falls within the MTSA 2002 guidelines and the state's security requirements. As with the two other ports profiled in this case study, due to the nature of the information and security vulnerabilities identified in the port's assessment, its FSP is unattainable.

In September 2007, a training exercise known as Operation Safe Passage, conducted by a joint task force, deployed officers from fifteen local, state, and federal law enforcement agencies to PortMiami. This exercise showed a unity of force by combined agencies from all levels of government and involved stringent security checks as well as additional X-ray scanner trucks and K-9 units.

Similar to PHA and PLB, PortMiami is one of thirty-five ports that participate in the TWIC program. The port has improved its security by implementing enhanced technology such as the Radar Surveillance and Automated Vessel Identification System. This system integrates a coastal tracking system with state-of-the-art radar technology and can detect ship-mounted transponders to identify and locate vessels by electronically exchanging data with nearby ships and Vessel Traffic Stations. The radar surveillance integrates both radar and automated vessel identification data to provide the highest visibility within the port complex. In addition, a new Video Management System designed for the high-end security market provides high-resolution video.

Although 100 percent of the cargo containers leaving PortMiami are scanned for radiation or nuclear material, the number of scanners currently operating in the port is unknown.

Federal Funding

PortMiami is categorized as Group II (moderate risk) by FEMA, which places it behind the seaports in Group I in terms of PSGP eligibility and funding priority. However, this does not detract from the port's importance, not only to southern Florida, but also to the southeastern region of the United States. PortMiami did not qualify for PSGP funding in FY 2013. Typically, port tenants and eligible recipients are advised to complete all qualification and application processes through an area-wide coordinating agent, in this case the Miami River Marine Group, in order to request funding for their specific security initiatives. However, as of 2013, the treasurer of Miami River Marine Group is serving house arrest on federal criminal charges of approving and directing the building of illegal docks. This incident caused distrust within the system and raised questions about PortMiami's ability to legally manage PSGP monies and opened further investigation into previous grant years. The hardest hit by this event are the beneficiaries of potential grant funds, including the port tenants and all local, state, and federal agencies that manage the port's safety and security.

Research Evaluation Criteria Chart

This research utilized a qualitative analysis approach for the three seaports and rated them as *completed*, *continuous*, *none*, and *N/A* (not available). Table 2 presents the

results of the case study conducted on PLB, PHA, and PortMiami and summarizes the information and data collected.

Table 2. Case Study Comparison Chart of the Ports of Long Beach, Houston, and Miami-Dade			
Evaluation Criteria	Port of Long Beach	Port of Houston	Port of Miami-Dade
Seaport Security Plans			
Local plans written	Completed	Completed	Completed
Local plans follow strategic guidance	Completed	Completed	Completed
Local government partners with private sector	Completed	Completed	Completed
Communication system in place	Completed	Completed	Completed
Physical security and access control	Continuous	Continuous	Continuous
Application of Guidelines			
Applied federal guidance within local plans	Completed	Completed	Completed
Applied legislation within local plans	Completed	Completed	N/A
Scheduled exercises conducted by local public and private sectors	Completed	Completed	N/A
Exercises met federal standards	Completed	Completed	N/A
Training conducted	Completed	Completed	Completed
Federal Funding			
Applied for federal grants	Completed	Completed	N/A
Budget allocated for technology research and development	None	None	None
Budget allocated for infrastructure improvement	Completed	Completed	None

Source: Created by author, adapted from Jenifer L. Breaux, “Seaport Protection Against Chemical and Biological Attacks” (Master’s thesis, U.S. Army, Command and General Staff College), 62.

Overall, each seaport has made tremendous improvements since 9/11 in enhancing its ability to secure its respective ports and deter and respond to a potential nuclear or radiological attack from a terrorist organization. Each port has implemented an FSP that is within the MTSA 2002 guidelines and 33 CFR 105 regulations, with each being assessed yearly by CBP and USCG. Each port has established a solid relationship with its local, state, and federal security partners to ensure that a common goal is determined and all entities are fully aware of their roles and responsibilities in regard to port security. In addition, each port has established a central location within its complex for all stakeholders to operate from and allow freedom of coordination and communication within all branches, to include the private sector. Both PLB and PHA hold annual homeland security exercises that include partners from all government levels, albeit lasting only a couple of days. Recent data on PortMiami's scheduled annual exercises that involve local, state, and federal agencies are not available. Although PortMiami interacts with entities from these agencies on a daily basis, there does not seem to be a major emphasis on conducting this type of training.

PLB and PHA are both categorized as Group I, high-risk seaports, giving them priority security funding through the PSGP. This allows these ports to be more aggressive in planning, implementing, and enhancing their security management and conducting training exercises compared to PortMiami, which is categorized as Group II. That a key figure within PortMiami, who was directly responsible for managing the funds is under house arrest for illegal usage of grant monies has cast a long shadow over the port's

operational abilities and has caused several questions to arise on how effectively the port has utilized its previous grant funding.

None of the seaports is currently invested in technology research and development to assist in the scanning and detection of nuclear or radiological materials, but each has participated in past pilot programs offered by DHS, including the TWIC program, which is in continuous use at each port. All three ports have volunteered to be part of the C-TPAT program and undergo security audits every four-years and biannual reviews from CBP audit teams.

Conclusion

This chapter focused on the research analysis of the thesis, using three major U.S. seaports as the case study. The analysis partially answered the primary question of the thesis: What are the current standard procedures for inbound cargo inspections in U.S. seaports, and which actions have been taken to meet the 2007 congressional directive for 100-percent inspection of weapons-grade nuclear and radioactive substances prior to departure from foreign seaports? Due to the nature of the study, attaining an actual FSP for each port was not possible due to DHS regulations and security breach protocols, but there is a certified security procedure in place for each port. CBP and USCG are actively involved in assessing and certifying each port's security processes. Protective measures have advanced significantly due to the PSGP, which has assisted in the continued improvement of the preparedness and response of each port.

Utilizing the evaluation chart distinguished the similarities and differences of each port's current standing. The following chapter will include the thesis summary, as well as conclusions and recommendations for U.S. seaport security.

¹Federal Emergency Management Agency, *National Preparedness Report* (Washington, DC: Government Printing Office, 2013), 1.

²U.S. Department of Transportation, "A Short History of the Maritime Administration," http://www.marad.dot.gov/about_us_landing_page/marad_aboutus_history/vessel_short_history/History_Maritime_Administration.htm (accessed May 20, 2014).

³U.S. Customs and Border Protection, *Securing America's Borders at Ports of Entry* (Washington, DC: Government Printing Office, 2011), 1.

⁴U.S. Customs and Border Protection, *Protecting America: 2005–2010 Strategic Plan* (Washington, DC: Government Printing Office, 2005), 1.

⁵Executive Office of the President of the United States, *The National Strategy for Maritime Security* (Washington, DC: Government Printing Office, 2012), 1.

⁶House Committee on Homeland Security, *Oversight Plan of the Committee on Homeland Security*, 113th Cong., 1st sess., 2013, H. Rep. 113-314, 1.

⁷*Ibid.*, 5.

⁸U.S. Government Printing Office, "Subchapter H—Maritime Security," <http://www.gpo.gov/fdsys/pkg/CFR-2010-title33-vol1/pdf/CFR-2010-title33-vol1-part101.pdf> (accessed May 21, 2014), 315.

⁹U.S. Government Printing Office, "33 U.S.C: Navigation and Navigable Waters," <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title33/html/USCODE-2011-title33-chap25-sec1226.htm> (accessed May 21, 2014).

¹⁰U.S. Congress, *Public Law 107–295: Maritime Transportation Security Act of 2002*, 107th Cong., 2d sess., 2002, H. Rep. 107-777, 4.

¹¹U.S. Customs and Border Protection, "C-TPAT: Customs-Trade Partnership Against Terrorism," <http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism> (accessed May 18, 2014).

¹²*Ibid.*

¹³U.S. Customs and Border Protection, “CSI: Container Security Initiative,” <http://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief> (accessed May 20, 2014).

¹⁴*Ibid.*

¹⁵World Shipping Council, “Operation Safe Commerce,” http://www.worldshipping.org/pdf/operation_safe_commerce.pdf (accessed May 21, 2014), 1.

¹⁶*Ibid.*, 5.

¹⁷U.S. Department of Transportation, “A Short History of the Maritime Administration.”

¹⁸National Nuclear Security Administration, “Megaports Initiative,” <http://nnsa.energy.gov/aboutus/ourprograms/nonproliferation/programoffices/internationalmaterialprotectionandcooperation/-5> (accessed May 21, 2014).

¹⁹*Ibid.*

²⁰U.S. Department of Transportation, “Port Security Grant Program (PSGP),” http://www.marad.dot.gov/ports_landing_page/infra_dev_congestion_mitigation/intermodal_transport_networks/intermod_trans_net_port_sec/PSGP.htm (accessed May 21, 2014).

²¹United States Government Accountability Office, “Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts,” <http://www.gao.gov/new.items/d05557.pdf> (accessed May 21, 2014), 4.

²²Jim Rowan, “TWIC - Present and Future Issues & Concerns,” <http://www.asishouston.org/ChapterNews/Speakers/ESC%20080608-TWIC%20Presentation%20-%20Jim%20Rowan.pdf> (accessed March 14, 2014), 5.

²³U.S. Department of Homeland Security, “United States Customs and Border Protections’ Radiation Portal Monitors at Seaports,” http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_SLP_13-26_Jan13.pdf (accessed May 21, 2014), 1.

²⁴“ASE Shows Cargo and Vehicle Inspection System,” *Homeland Security News Wire*, October 4, 2009, <http://www.homelandsecuritynewswire.com/ase-shows-cargo-and-vehicle-inspection-system> (accessed May 21, 2014).

²⁵Zachary Horowitz, “Applications of Radio Frequency Identification Technology to Container and Security Tracking,” http://web.cecs.pdx.edu/~monserec/courses/freight/classprojects/PDF%20-%20rfid_in_container_security_paper.pdf (accessed May 21, 2014), 2.

²⁶Port of Houston Authority, “Port Security and Emergency Operations,” http://www.deepeningportofhouston.com/downloads/fact_sheets/PHA-DW-Security.pdf (accessed May 18, 2014), 21.

²⁷Port of Houston Authority, “Sunset Advisory Commission: Staff Report,” <http://www.portofhouston.com/inside-the-port-authority/government-relations/sunset-review/> (accessed May 18, 2014).

²⁸Jim Herron Zamora, “California Lists Top Terror Targets/Airports, bridges, Stadiums on Secret List,” *SFGate*, February 23, 2003, <http://www.sfgate.com/news/article/California-lists-top-terror-targets-Airports-2631969.php> (accessed May 18, 2014).

²⁹Port of Long Beach, “Customs - Trade Partnerships Against Terrorism,” http://www.polb.com/about/security/c_tpat.asp (accessed March 22, 2014).

³⁰Port of Long Beach, “Port Continues to Strengthen Security,” <http://www.polb.com/news/displaynews.asp?NewsID=1062> (accessed March 21, 2014).

³¹Florida’s Domestic Oversight Council, “2013 Domestic Security Annual Report,” <http://www.fdle.state.fl.us/Content/getdoc/e709667e-abcd-4a4a-99f3-a5b50de9d135/2013-DS-Annual-Report-Final.aspx> (accessed May 18, 2014), 34–37.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

The level of security granted to U.S. seaports will depend on the initiative and active participation of private sector entities as well as local, state, and federal governments. All stakeholders will play an important role in the continued protection of U.S. interests involving the maritime domain. Chapter 4 researched and analyzed the laws, policies, and regulations implemented for seaport security, as well as the current technology in place. Although significant improvements have been made since 9/11, the analysis of the Houston, Miami-Dade, and Long Beach seaports further supports the continuous need for advancements in streamlining security processes and technology use. Moreover, additional homeland security exercises must be conducted each year to assess current security measures and their ability to deter and respond to the evolving nuclear and radiological threat of a dirty bomb hidden in a cargo container bound for the United States. Foremost, the data analysis answered the primary and secondary thesis questions. Based on Chapter 4 findings, this chapter will discuss the research conclusions and provide recommendations for future port security and its ability to deter a WMD, in this case a dirty bomb.

Primary Research Question

The primary question of this thesis is: What are the current standard procedures for inbound cargo inspections in U.S. seaports, and which actions have been taken to meet the 2007 congressional directive for 100-percent inspection of weapons-grade nuclear and radioactive substances prior to departure from foreign seaports? A general

answer can be provided for the primary question: there are mandated and regulated standard operating procedures required of all U.S. seaports, written in each port's FSP, which is annually reviewed and audited by USCG. The FSP details, by category, the standard requirements for each facility concerning all aspects of port security. Although all seaports must follow the guidelines set by the MTSA 2002 and 33 CFR 105, it is possible that additional state regulations can be added to the security procedure for a more stringent security system, provided that the federal mandates are covered. Because the FSPs—the actual security processes—for the three seaports analyzed in the case study were unobtainable, information is not available to reveal the current procedures in place to more specifically answer, with detailed information, the first part of the thesis question.

The second part of the thesis question is: Which actions have been taken to meet the 2007 congressional directive for 100-percent inspection of weapons-grade nuclear and radioactive substances prior to departure from foreign seaports? Since the 2007 congressional directive for 100-percent inspection, fifty-eight CSI ports in thirty-two countries have been established as of July 2013. However, these ports account for only 80 percent of all cargo containers shipped to the United States; cargo containers leaving these ports have not necessarily been inspected by a nuclear or radiological scanner prior to being loaded on a vessel bound for the United States.

Secondary Research Questions

Further analysis of the research allows the secondary research questions to be answered and supports the answers given to the primary question.

1. If standards have been improved since the MTSA 2002, will they detect and prevent a nuclear dirty bomb device from reaching a major seaport? The two major federal agencies leading this effort are CBP and USCG. These agencies continually promote a multilayered and domain-awareness approach when it comes to maritime security. However, without additional information on these two approaches, it is difficult to pinpoint exactly how these agencies can detect and prevent a dirty bomb from reaching a major U.S. seaport. It is known that these methods include reliance on the intelligence community composed of the Federal Bureau of Investigation, the Central Intelligence Agency, the Department of Defense, the NSA, and other federal intelligence agencies whose focus and mission is to deter a nuclear catastrophe in the United States caused by a terrorist organization.
2. What current technology is available to screen a higher percentage of cargo containers bound for the United States? This question may be better rewritten as: Does the United States have enough technology in place to screen a higher percentage of cargo containers bound for the United States? The answer then would be yes, there is technology in place to screen inbound cargo containers. However, it cannot ensure coverage around the world and to all participating CSI ports. This includes trained personnel to operate and maintain the equipment.
3. Is the United States—specifically DHS—prepared for future terrorist attacks originating from inbound cargo containers? DHS has several established

strategies in place, from the national to the interagency levels, to conceptually deter, respond to, and recover from a dirty bomb attack in a U.S. seaport. The greater question is whether DHS has the resources to execute the plans in place. This problem lies mainly with the annual budget allocated to DHS, including PSGP funding allotments.

4. Is it feasible to conduct 100-percent inspection of all U.S.-bound cargo containers? With nearly 11.5 million cargo containers entering the United States annually, it is not feasible to conduct 100-percent inspection of all U.S.-bound cargo containers. Such a feat would not only hinder the flow of goods to the United States, thus hurting the nation's economy, but would also require a tremendous amount of financial resources that the government cannot afford, especially with expected budgetary cutbacks for maritime security initiatives in the near future. Continued reliance on the multilayered and domain awareness approach will be necessary to mitigate risks from unscanned containers bound for the United States.

Overview of Summary of Research

An overview of the research will substantiate the answers given to both the primary and secondary thesis questions. A brief summary of each section will provide a general understanding of and correlation to the answers for the primary and secondary questions.

Case Analysis

Analysis of the three ports revealed that each has made progress since 9/11. They continue to work closely with their security partners at the local, state, and federal levels to ensure that their FSPs are in compliance with federal regulations. The comparison evaluation chart included topics that summarized each port's progress in and efforts made to advance their respective seaport security programs. Each port operates differently from one another and has its own specific strengths and vulnerabilities.

Security Plans

Although actual FSPs and USCG assessments for the three seaports were unobtainable, they all fall within federal guidelines. In addition, some ports also have mandated state homeland security directives that must be followed, to include federal mandates.

Current Protective Measures

Each of the three ports has protective measures in place to prevent unauthorized personnel and vessels from moving about within its facility. From the implementation of the TWIC program to the installation of updated high-definition cameras, each port has enhanced its protective measures. In addition to the local, state, and federal law enforcement agencies assigned to the ports, all three have a Maritime Security Response Team, composed of a staff of seventy-five personnel capable of responding to chemical, biological, radiological, nuclear, or explosive threats.

Funding

The PSGP plays an important role in assisting with the implementation of the National Preparedness System by supporting the construction, maintenance, and delivery of its core capabilities, resulting in a secure and resilient nation. Funding from the PSGP supports maritime security through prevention, protection, mitigation, response, and recovery missions.

In FY 2013, the PSGP awarded more than \$93 million for infrastructure security activities to implement maritime and FSPs within the port authorities, facility operators, and state and local government agencies required to provide U.S. port security services. The intent of the program is to award grant funding to eligible applicants (U.S. seaports) in order to support increased port-wide risk management; enhance domain awareness; conduct training and exercises; expand port recovery and resiliency capabilities; and further capabilities to prevent, detect, respond to, and recover from attacks involving radiological or nuclear materials, as well as other conventional methods.¹

The three ports chosen for this case study have all been active applicants of the grant program since its inception in FY 2002. The funding was directed toward immediate security programs that were required to meet the MTSA 2002 mandate. U.S. seaports are categorized in groups (I through IV) with the first group designated as high-risk ports. Both PLB and PHA have Group I designations and receive priority funding from the PSGP annual budget. PortMiami is in Group II, which is the second group to have priority in requests for grant funding. It is evident from the case study findings that both PLB and PHA have fully taken advantage of their PSGP funding. Since 2002, both ports have enhanced their security protocols with the implementation of new technology,

ranging from TWIC programs, additional nuclear and radiological scanners, updated cameras and monitors, and joint exercises for all levels of government, to include the private sector. PortMiami, while operating within federal regulation, also took advantage of PSGP opportunities and increased its security posture with improvements to its security process and upgrades to its security technology. However, due to recent allegations of misappropriated PSGP grant monies, FY 2013 grant funding was not awarded to PortMiami, thus causing a delay in the port's progress to meet its goal of enhanced port security. In addition, previous years' PSGP awards are now being reviewed for legitimate appropriations.

For FY 2014, \$100 million will be available for the PSGP to directly support maritime transportation infrastructure security activities.² Although these resources may seem adequate to improve U.S. seaport security initiatives, they are not nearly enough to support the top 150 ports (to include river ports) in the United States. Moreover, pending budget cutbacks in PSGP funding may potentially undo progress made in past years.

Meaning of Findings

Under the guidance and direction of DHS, as well as local, state, and federal entities, U.S. seaports have made tremendous gains in improving security measures since the 9/11 attacks. Regulations and security initiatives mandated by the MTSA 2002 for greater coordination and information sharing between law enforcement agencies at all levels has increased, and annual homeland security exercises have been implemented to assess these agencies' ability to deter, respond to, and recover from a catastrophic event. In addition to the difficulty of allocating resources and manpower from all levels of

government to attend an annual exercise, a two-day training is an insufficient amount of time to assess current personnel, equipment, and security procedures.

The increased security measures implemented in the seaports have made it difficult for unauthorized personnel and vehicles to enter and have freedom of movement without being compromised. Safety zones designated and patrolled by both the Harbor Patrol and USCG deny unauthorized maritime vessels from reaching restricted areas. Nearly 100 percent of cargo containers leaving U.S. seaports are scanned for radiological and nuclear substances prior to departure to their final destinations within the United States. However, the problem continues to persist outside of the United States as the 2007 congressional mandate requiring 100-percent scanning of U.S.-bound cargo containers for radiological and nuclear substances by 1 July 2012 was not met, as reported by the Government of Accountability Office in its review of maritime security in 2012.³ At present, fifty-eight seaports around the world participate in the CSI. However, cargo containers coming from these ports account for only 80 percent of the shipments that arrive in the United States; the remaining 20 percent originate from ports that are not CSI participants. Even more alarming, it was reported in 2012 that, on average, 5 percent of U.S.-bound cargo containers are scanned annually, almost no different from the 2007 statistics.⁴ To help account for these statistics, prior to the start of the CSI program, former DHS Secretary Janet Napolitano stated that the program was possible on only a limited scale; the major challenge would be expanding to all seven hundred international maritime ports that handle U.S.-bound cargo containers daily.⁵ Current and future budget cutbacks to these security initiatives will further limit the scanning technology DHS can

provide, as well as the amount of qualified personnel who can be trained to operate and maintain this equipment. The former secretary offered a more feasible alternative to securing the U.S. supply chain by suggesting the use of a risk-based approach, which would focus on analyzing cargo characteristics and place of origin in order to identify high-risk cargo, resulting in further inspection.⁶

Recommendations

It is evident that U.S seaport security has improved through enhanced technology and security agency partnerships at all levels of government. But the weakness lies outside the United States, from the point of origin of inbound cargo containers. Currently, there are fifty-eight ports worldwide that participate in the CSI program, but that does not necessarily mean that every container is scanned. The program's intent is to deter a cargo container carrying radiological or nuclear materials from entering a U.S. seaport. If cargo of this type reaches the U.S. mainland, it has already met its goal. If this were to happen, no matter how stringent internal port security may be, it would all be for naught. The recommendations made for this research include: funding allocations, Department of Defense assistance, exercises and training, research and development, and global partnerships.

Funding Allocations

The key to deterring successful detonation of a dirty bomb in a U.S. seaport is to find and stop it from its point of origin. An inbound cargo container that slips through the U.S. external maritime security measures is one that has already accomplished its mission. Continued funding for the CSI program and the Megaports Initiative is required

to maximize the nation's ability to deter this threat. If need be, reducing annual PSGP awards in order to reallocate funds to overseas initiatives may be a better use of these funds to solve this problem.

Department of Defense Assistance

With the war in Afghanistan winding down by the end of 2014, utilizing military forces to assist with homeland security is a viable option. The military has the resources and capability to handle chemical, biological, radiological, nuclear, and explosive matters. Even if this does not become a future mission for the U.S. military, it will serve as a valuable training opportunity for any Defense Support of Civil Authorities missions that may arise.

Exercise and Training

Although it was noted that the three ports conduct annual homeland security exercises, these brief trainings are not nearly enough to sufficiently assess each port's current FSP and the responders' capabilities. Additional guidance and directives are required from DHS to institute quarterly training exercises involving high-risk ports. It is imperative that the exercises meet the current threat environment and be as realistic as possible. However, conducting an exercise of this magnitude four times each year will require the port, or portions of it, to become inoperable during the exercise, meaning money lost during the down time.

Research and Development

Not a lot of emphasis has been placed on the research and development of new technology that can assist with the scanning of cargo containers. Developing new technology that is lighter, more cost effective, and thorough will be necessary if attaining 100-percent cargo inspection remains the ultimate goal.

Global Partnerships

Continued collaborations with and mutual understanding of the goals between the United States and its international trade partners will be necessary to continuously protect the global supply chain, benefitting everyone. Initiatives that support the training of overseas partners and equip them with the necessary tools to effectively implement security initiatives will not only need to remain in place but increase in support.

Conclusions

In December 2001, Osama bin Laden's Deputy, Ayman Zawahiri, stated, "If you have US\$30 million, go to the black market in central Asia, contact any disgruntled Soviet scientist and a lot of dozens of smart briefcase bombs are available"; a few months later, Al-Qaeda announced its goal to "kill four million Americans."⁷ The constant threat of a terrorist organization detonating a radiological or nuclear device in one of America's 361 seaports should serve as a reminder that the aviation industry should not be the sole focus of all security improvements. U.S. seaports are a major part of the country's economic lifeline and a considerable aspect of maritime and homeland security. A dirty bomb attack on a major U.S. seaport will not only destroy critical infrastructure and kill

numerous personnel, but the port's inoperability will cost the country billions of dollars each day, as well as affect the people's trust in the government's ability to protect them.

The ports of Long Beach, Houston, and Miami-Dade are examples of high- to moderate-risk ports that require federal attention. They all have received numerous grant awards through the PSGP. They have made great strides in improving their internal security. However, this does not change the fact that an inbound cargo container carrying a dirty bomb that slips through a port's layered defense makes the internal security irrelevant.

The results of this case study verified that the security standards set by the federal government are followed by these three ports and are annually reviewed by federal agencies to ensure proper compliance. Funding provided by the PSGP plays a major role in enhancing security measures to all eligible applicants, and, at this time, continues to fund future security initiatives. It must be kept in mind that due to the U.S. economic situation, future DHS budgetary cutbacks are inevitable and progress made in past years will slowly deteriorate.

Continued collaboration among all security partners from local, state, federal, and private entities has improved. These agencies must continue to be proactive in advancing their security plans and procedures to meet ever-changing threats. The inability to scan for radiological and nuclear substances in 100 percent of U.S.-bound cargo containers should be mitigated by continued partnership building across the globe. Allocating resources and prioritizing potential threats from point of origin ports will require significant thought and action from U.S. policymakers and security agencies.

¹Federal Emergency Management Agency, “FY 2013 Port Security Grant Program (PSGP),” <http://www.fema.gov/fy-2013-port-security-grant-program-psgp-0> (accessed May 18, 2014).

²Federal Emergency Management Agency, “FY 2014 Port Security Grant Program (PSGP),” <http://www.fema.gov/fy-2014-port-security-grant-program-psgp> (accessed May 21, 2014).

³Ben Bain, “DHS to Miss 2012 Deadline to Scan Containers for Radiation,” *FCW*, December, 2 2009, <http://fcw.com/Articles/2009/12/02/DHS-cargo-radiation-scanning-extension.aspx?Page=1> (accessed May 18, 2014).

⁴Nathan Donahue, “Inherent Security at U.S. Ports,” Center for Strategic and International Studies, <http://csis.org/blog/inherent-insecurity> (accessed March 21, 2014).

⁵Douglas Frantz, “Port Security: U.S. Fails to Meet Deadline for Scanning Cargo Containers,” *The Washington Post*, July 15, 2012, http://www.washingtonpost.com/world/national-security/port-security-us-fails-to-meet-deadline-for-scanning-of-cargo-containers/2012/07/15/gJQAmgW8mW_story.html (accessed January 22, 2014).

⁶James Jay Carafano and Jessica Zuckerman, “Maritime Cargo Scanning Folly: Bad for the Economy, Wrong for Security,” The Heritage Foundation, <http://www.heritage.org/research/reports/2012/02/maritime-cargo-port-security-and-the-100-percent-screening-mandate> (accessed May 18, 2014).

⁷Australian Associated Press, “Journalist Says Al-Qaeda Has Black Market Nuclear Bombs,” *The Sydney Morning Herald*, March 22, 2004, <http://www.smh.com.au/articles/2004/03/22/1079823250899.html> (accessed May 18, 2014).

BIBLIOGRAPHY

- “33 U.S.C: Navigation and Navigable Waters.” <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title33/html/USCODE-2011-title33-chap25-sec1226.htm> (accessed May 21, 2014).
- “ASE Shows Cargo and Vehicle Inspection System.” *Homeland Security News Wire*, October 4, 2009. <http://www.homelandsecuritynewswire.com/ase-shows-cargo-and-vehicle-inspection-system> (accessed May 21, 2014).
- Australian Associated Press. “Journalist Says Al-Qaeda Has Black Market Nuclear Bombs.” *The Sydney Morning Herald*, March 22, 2004. <http://www.smh.com.au/articles/2004/03/22/1079823250899.html> (accessed May 18, 2014).
- Bain, Ben. “DHS to Miss 2012 Deadline to Scan Containers for Radiation.” *FCW*, December, 2 2009. <http://fcw.com/Articles/2009/12/02/DHS-cargo-radiation-scanning-extension.aspx?Page=1> (accessed May 18, 2014).
- Bliss, Jeff. “U.S. Backs Off All-Cargo Scanning Goal with Inspections at 4%.” *Bloomberg*, August 13, 2012. <http://bloom.bg/MTFVZ1> (accessed April 22, 2014).
- Breaux, Jenifer L. “Seaport Protection Against Chemical and Biological Attacks.” Master’s thesis, U.S. Army, Command and General Staff College, 2009.
- Carafano, James Jay, and Jessica Zuckerman. “Maritime Cargo Scanning Folly: Bad for the Economy, Wrong for Security.” The Heritage Foundation. <http://www.heritage.org/research/reports/2012/02/maritime-cargo-port-security-and-the-100-percent-screening-mandate> (accessed May 18, 2014).
- Chen, Michael. “Development in Maritime and Supply Chain Security.” <http://www.iaphworldports.org/LinkClick.aspx?fileticket=x8Wf2KcuFD0%3D&tabid=5609> (accessed February 26, 2014).
- Congressional Port Security Caucus. *A Report on Port and Maritime Security: An Agenda to Enhance America’s Security*. Washington, DC: Government Printing Office, 2007.
- Donahue, Nathan. “Inherent Security at U.S. Ports.” Center for Strategic and International Studies. <http://csis.org/blog/inherent-insecurity> (accessed March 21, 2014).
- Executive Office of the President of the United States. *National Security Strategy*, May 2010. <http://nssarchive.us/NSSR/2010.pdf> (accessed January 22, 2014).

- . *The National Strategy for Maritime Security*. Washington, DC: Government Printing Office, 2012.
- Federal Emergency Management Agency. “FY 2013 Port Security Grant Program (PSGP).” <http://www.fema.gov/fy-2013-port-security-grant-program-psgp-0> (accessed May 18, 2014).
- . “FY 2014 Port Security Grant Program (PSGP).” <http://www.fema.gov/fy-2014-port-security-grant-program-psgp> (accessed May 21, 2014).
- . *National Preparedness Report*. Washington, DC: Government Printing Office, 2013.
- Florida’s Domestic Oversight Council. “2013 Domestic Security Annual Report.” <http://www.fdle.state.fl.us/Content/getdoc/e709667e-abcd-4a4a-99f3-a5b50de9d135/2013-DS-Annual-Report-Final.aspx> (accessed May 18, 2014).
- Flynn, Stephen E. “The Neglected Home Front.” *Foreign Affairs* (September/October 2004). <http://www.mafhoum.com/press7/207P8.htm> (accessed November 22, 2013).
- Frantz, Douglas. “Port Security: U.S. Fails to Meet Deadline for Scanning Cargo Containers.” *The Washington Post*, July 15, 2012. http://www.washingtonpost.com/world/national-security/port-security-us-fails-to-meet-deadline-for-scanning-of-cargo-containers/2012/07/15/gJQAmgW8mW_story.html (accessed January 22, 2014).
- Frittelli, John F. *Maritime Security: Overview of Issues*, Congressional Research Service Report for Congress RS21079. Washington, DC: Library of Congress, 2003.
- GlobalSecurity.org. “Al-Qaeda (The Base).” <http://www.globalsecurity.org/military/world/para/al-qaida.htm> (accessed May 20, 2014).
- . “Osama bin Laden.” http://www.globalsecurity.org/security/profiles/osama_bin_laden.htm (accessed May 20, 2014).
- Homeland Security Council. “National Strategy for Homeland Security.” http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (accessed January 22, 2014).
- Horowitz, Zachary. “Applications of Radio Frequency Identification Technology to Container and Security Tracking.” http://web.cecs.pdx.edu/~monserec/courses/freight/classprojects/PDF%20-%20rfid_in_container_security_paper.pdf (accessed May 21, 2014).

House Committee on Homeland Security. *Oversight Plan of the Committee on Homeland Security*. 113th Cong., 1st sess., 2013, H. Rep. 113-314.

Jones, Susan. "Intelligence Chair Warns of 'New Bombs, Very Big Bombs.'" *CNSnews.com*, December 2, 2013. <http://cnsnews.com/news/article/susan-jones/intelligence-chairs-warn-new-bombs-very-big-bombs> (accessed February 26, 2014).

Maritime Transport Committee. "Security in Maritime Transport: Risk Factors and Economic Impact." <http://www.oecd.org/sti/transport/maritimetransport/18521672.pdf> (accessed January 22, 2014).

National Nuclear Security Administration. "Megaports Initiative." <http://nnsa.energy.gov/about/ourprograms/nonproliferation/programoffices/internationalmaterialprotectionandcooperation/-5> (accessed May 21, 2014).

National Security Strategy Archive. "The National Security Strategy Report." <http://nssarchive.us> (accessed May 20, 2014).

Port of Houston Authority. "Port Security and Emergency Operations." http://www.deepeningportofhouston.com/downloads/fact_sheets/PHA-DW-Security.pdf (accessed May 18, 2014).

———. "Sunset Advisory Commission: Staff Report." <http://www.portofhouston.com/inside-the-port-authority/government-relations/sunset-review/> (accessed May 18, 2014).

Port of Long Beach. "Customs - Trade Partnerships Against Terrorism." http://www.polb.com/about/security/c_tpat.asp (accessed March 22, 2014).

———. "Port Continues to Strengthen Security." <http://www.polb.com/news/displaynews.asp?NewsID=1062> (accessed March 21, 2014).

Port Security Council. *Port Security Is Our National and Economic Security: Fact Sheet*. Washington, DC: Government Printing Office, 2006.

Romo, Rafael, Nick Parker, and Mariano Castillo. "Mexico: Stolen Radioactive Material Found." *CNN News*, December 4, 2013. <http://www.cnn.com/2013/12/04/world/americas/mexico-radioactive-theft> (accessed April 23, 2014).

Rowan, Jim. "TWIC - Present and Future Issues & Concerns." <http://www.asishouston.org/ChapterNews/Speakers/ESC%20080608-TWIC%20Presentation%20-%20Jim%20Rowan.pdf> (accessed March 14, 2014).

Sherman, Rexford B. *Seaport Governance in the United States and Canada*. Alexandria, VA: American Association of Port Authorities, 2012.

“Subchapter H—Maritime Security.” <http://www.gpo.gov/fdsys/pkg/CFR-2010-title33-vol1/pdf/CFR-2010-title33-vol1-part101.pdf> (accessed May 21, 2014).

Transportation Security Administration. “Our Workforce.” <http://www.tsa.gov/about-tsa/our-workforce> (accessed May 20, 2014).

United States Government Accountability Office. “Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts.” <http://www.gao.gov/new.items/d05557.pdf> (accessed May 21, 2014).

———. “Maritime Security: DHS Progress and Challenges in Key Areas of Port Security.” <http://www.gao.gov/assets/130/125051.pdf> (accessed May 20, 2014).

———. “Maritime Security: Progress and Challenges 10 Years after the Maritime Transportation Security Act.” <http://www.gao.gov/assets/650/647999.pdf> (accessed January 22, 2014).

———. “Supply Chain Security: Container Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning.” <http://www.gao.gov/assets/590/588253.pdf> (accessed May 20, 2014).

U.S. Congress. House. *Improving America’s Security Act of 2007*. 110th cong., 1st sess., July 9, 2007.

———. *Oversight Plan of the Committee on Homeland Security*. 113th Cong., 1st sess., January 3, 2013.

———. *Public Law 107-295: Maritime Transportation Security Act of 2002*. 107th Cong., 2d sess., November 25, 2002.

U.S. Congress. Senate. *Committee on Homeland Security and Governmental Affairs. Statement for the Record, Acting Secretary Rand Beers, U.S. Department of Homeland Security*, November 14, 2013.

U.S. Customs and Border Protection. *Container Security Initiative in Summary*. Washington, DC: Government Printing Office, 2011.

———. “CSI: Container Security Initiative.” <http://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief> (accessed May 20, 2014).

———. “C-TPAT: Customs-Trade Partnership Against Terrorism.” <http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism> (accessed May 18, 2014).

- . *Protecting America: 2005–2010 Strategic Plan*. Washington, DC: Government Printing Office, 2005.
- . *Securing America's Borders at Ports of Entry*. Washington, DC: Government Printing Office, 2011.
- U.S. Department of Homeland Security. "Department of Homeland Security Strategic Plan: Fiscal Years 2012–2016." <http://www.hsdl.org/?view&did=700830> (accessed May 20, 2014).
- . *Maritime Security Infrastructure Recovery Plan for the National Strategy for Maritime Security*. Washington, DC: Government Printing Office, 2005.
- . "National Response Framework." 2nd ed. http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf (accessed February 26, 2014).
- . "Radiological Attack: What It Is." <http://www.dhs.gov/radiological-attack-what-it> (accessed May 20, 2014).
- . "Ten Years Later: A Stronger, Safer America." <http://www.dhs.gov/blog/2011/09/11/ten-years-later-stronger-safer-america> (accessed May 20, 2014).
- . "United States Customs and Border Protections' Radiation Portal Monitors at Seaports." http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_SLP_13-26_Jan13.pdf (accessed May 21, 2014).
- U.S. Department of Transportation. "A Short History of the Maritime Administration." http://www.marad.dot.gov/about_us_landing_page/marad_about_us_history/vessel_short_history/History_Maritime_Administration.htm (accessed May 20, 2014).
- . "Port Security Grant Program (PSGP)." http://www.marad.dot.gov/ports_landing_page/infra_dev_congestion_mitigation/intermodal_transport_networks/intermod_trans_net_port_sec/PSGP.htm (accessed May 21, 2014).
- World Shipping Council. "Operation Safe Commerce." http://www.worldshipping.org/pdf/operation_safe_commerce.pdf (accessed May 21, 2014).
- Zamora, Jim Herron. "California Lists Top Terror Targets/Airports, bridges, Stadiums on Secret List." *SFGate*, February 23, 2003. <http://www.sfgate.com/news/article/California-lists-top-terror-targets-Airports-2631969.php> (accessed May 18, 2014).